ATIS STANDARD

ATIS-1000112.2005

SIGNALING SYSTEM NUMBER 7 (SS7) – SIGNALING CONNECTION CONTROL PART (SCCP)

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

The Alliance for Telecommunication Industry Solutions (ATIS) is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from more than 350 communications companies are active in ATIS' 23 industry committees and its Incubator Solutions Program.

< http://www.atis.org/ >

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith.

ATIS-1000112.2005, *Signaling System Number 7 (SS7) – Signaling Connection Control Part (SCCP)*

Is an American National Standard developed by the **Interoperability (IOP) Subcommittee** under the **ATIS Packet Technologies and Systems Committee (PTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-1000112.2005

(Revision of T1.112-2001)

American National Standard for Telecommunications

Signaling System Number 7 (SS7) -- Signaling Connection Control Part (SCCP)

Secretariat

Alliance for Telecommunications Industry Solutions

Approved July 15, 2005

American National Standards Institute, Inc.

Abstract

This recommendation contains a general description of the services provided from the Message Transfer Part (MTP) of Signaling System Number 7 (SS7), the functions within the Signaling Connection Control Part (SCCP), and the resultant services provided for the users of the SCCP.

FOREWORD

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the standard.

This document is entitled "American National Standard for Telecommunications - Signaling System Number 7 (SS7) - Signaling Connection Control Part." It was originally based on the 1988 Blue Book specification of Signaling System No. 7 (SS#7) for international use, issued by the CCITT Study Group XI (Vol. VI, Fascicles VI.7 and VI.8) and is intended to be generally compatible with that standard and its successors. It has been appropriately modified for use within and between U.S. networks to meet the anticipated needs and applications of such entities. These modifications are the result of extensive work by the members of the PTSC-IOP (formerly T1S1.3) Working Group on U.S. Standards for Common Channel Signaling. In general, these modifications fall into two categories:

1) The specification of options designated by the ITU-T (formerly CCITT) for national use,
2) Extensions to the 1996 protocol to provide for new applications of the SS7 protocol. This is in accordance with current and projected ITU-T activity.

A vertical bar (|) in the right-hand margin indicates a change from the previous issue of this standard.

Note that the standard numbering has changed in this version of ATIS-1000111, ATIS-1000112, and ATIS-1000113. These standards were formerly numbered as T1.111, T1.112, and T1.113 respectively. The associated chapter numbering has not been modified.

This standard contains the following six chapters:

Changes and additions incorporated into these specifications consist of the following:

- Addition of new Translation Type Code "18" for ECS Call Routing.

The overall and detailed organization of these specifications parallels that used in the equivalent ITU-T Recommendations. Thus ATIS-1000112.1 through ATIS-1000112.5 of this standard correspond to Recommendations Q.711 through Q.714 and Q.716 of the ITU-T specification. ATIS-1000112.6 corresponds to Q.715.

This standard is intended for use in conjunction with T1.110-1999 (R2005), *Signaling System Number 7 (SS7) - General information*, which includes an overview of SS7, a glossary, and a chapter on abbreviations.

Information contained in a normative annex in these specifications is considered part of this standard.

Information contained in an informative annex in these specifications is not considered part of this standard but is rather auxiliary to the standard. Similarly, footnotes are not part of this official standard.

Caution should be exercised in using the Specification and Description Language (SDL) diagrams to interpret the standard; please note that the text always takes precedence over the SDL.

Future control of this document will reside with Accredited Standards Committee on Telecommunications, Alliance for Telecommunications Industry Solutions. This control of additions to the specification, such as ongoing protocol evolution, new applications, and operational requirements, will permit compatibility among U. S. networks. Such additions will be incorporated in an orderly manner with due consideration to the ITU-T layered model principles, conventions, and functional boundaries.

Suggestions for improvement of this standard will be welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, 1200 G Street, NW, Suite 500, Washington, DC 20005.

This standard was processed and approved for submittal to ANSI by the Accredited Standards Committee Packet Technologies and Systems Committee (PTSC). Committee approval of this standard does not necessarily imply that all committee members voted for its approval. At the time it approved this standard, the PTSC had the following members:

B. Hall, PTSC Chair
J. Zebarth, PTSC Vice-Chair
S. Carioti, ATIS Disciplines
S. Barclay, ATIS Secretariat
C. Underkoffler, ATIS Chief Editor
C. Brownmiller, ATIS Technical Editor
R. Singh, PTSC Technical Editor

Organization Represented	Name of Representative
AcmePacket	Kevin Klett
Alcatel USA Inc.	Ken Biholar
AT&T	Martin Dolly George Stanek (Alt)
BellSouth	Rick McNealy
BellSouth Telecommunications	David M. Brady
C.S.I Telecommunications	Michael S. Newman Thomas G Croda (Alt)
Cingular Wireless LLC	Don Zelmer Marc Grant (Alt)
Cisco Systems	Rajiv Kapoor Chip Sharp (Alt)
Defense Info. Systems Agency	Chris Fitzgerald Ryan Kuseki (Alt)
Ericsson Incorporated	Susana Sabater-Maroto Stephen Hayes (Alt)
FBI ESTS	Gregory Milonovich Eric Mason (Alt)
Harris Corporation	Marlis Humphrey
Hewlett-Packard	Steve Mills
Intelsat	Mark T. Neibert
Lucent Technologies	Stuart O. Goldman
MCI	J. Martin Carroll Robert Schafer (Alt)
National Communications Systems	Nicholas Andre Jean Trakinat (Alt)
Nokia Telecommunications Inc.	Joyabrata Mukherjee Ed Ehrlich (Alt)
Nortel	Joseph A. Zebarth
Qwest	Steve Showell Michael Fargano (Alt)
SBC Communications, Inc.	B.S. Sambasivan Bob Hall (Alt)
Siemens Communications, Inc.	Ron Franks David E. Francisco
Sprint Corporation	Mark L. Jones
Telcordia Technologies	Wesley Downum Cliff Halevi (Alt)
Tellabs Operations, Inc.	William A. Walker
Tridea Works	Greg Ratta
Verizon Communications	Dave Morris Wendy Pugh (Alt)

The Interoperability (IOP) Subcommittee was responsible for the development of this document.

TABLE OF CONTENTS

American National Standard for Telecommunications –

Signaling System Number 7 (SS7) -- Signaling Connection Control Part (SCCP)

ACRONYMS & ABBREVIATIONS

AC	Authentication Center
AI	Address Indicator
AIN	Advanced Intelligent Network
AK	Data Acknowledgment
ANSI	American National Standards Institute
AP	Application Process
ATIS	Alliance for Telecommunications Industry Solutions
BCD	Binary-Coded-Decimal
B-ISDN	Broadband Integrated Services Digital Network
CC	Connection Confirm or Country Code
CCITT	International Telegraph and Telephone Consultative Committee
CCS	Common Channel Signaling
CdPA	Called Party Address
CIID	Call Issuer ID
CNAM	Calling Name Delivery
CR	Connection Request
CREF	Connection Refused
CSC	Coordinated State Change
DPC	Destination Point Code
DT1	Data Form 1
DT2	Data Form 2
EA	Expedited Data Acknowledgment
ED	Expedited Data
EIA	Electronic Industries Association
EIR	Equipment Identification Register
EOP	End of Optional Parameters
ERR	Protocol Data Unit Error
ES	Encoding Scheme
GMSC	Gateway Mobile Switching Center
GPRS	General Packet Radio Service
GSM	Global System for Mobile
GTA	Global Title Address
GTAI	Global Title Address Information
GTT	Global Title Translation
HLR	Home Location Register
ICN	Interconnecting CCS Networks
IEC	International Electrotechnical Commission
IIF	Interworking and Interoperability Function
IIN	Issuer Identification Number
IMSI	International Mobile Station Identity
IN	Intelligent Network
INS	Intermediate Network Selection
IRI	ISNI Routing Indicator
ISDN	Integrated Services Digital Network
ISNI	Intermediate Signaling Network Identification
ISO	International Organization for Standardization
ISTP	International Signaling Transfer Point
ISUP	ISDN User Part
IT	Inactivity Test
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
LRN	Location Routing Number
LSB	Least Significant Bit
LUDT	Long Unitdata
LUDTS	Long Unitdata Service
MAN	Mandatory Field
MAP	Mobile Application Part

MC	Message Center
MCC	Mobile Country Code
MDN	Mobile Directory Number
MI	Mark for Identification Indicator
MII	Major Industry Identifier
MIN	Mobile Identification Number
MNC	Mobile Network Code
MSC	Mobile Switching Center
MSIN	Mobile Station Identification Number
MSISDN	Mobile Station International ISDN Number
MSS	Message Storage System
MSU	Message Signal Unit
MTI	Message Type Interworking
MTP	Message Transfer Part
MTP-3	Message Transfer Part level 3
NANP	North American Numbering Plan
NDC	National Destination Code
NE	Network Entity
NID	Network Identifiers
NP	Number Portability or Numbering Plan
NPA	Numbering Plan Area
NPCI	Network Protocol Control Information
NPDU	Network Protocol Data Unit
NSDU	Network Service Data Units
NSL	Network Service Layer
NSP	Network Service Part or Network Service Provider
NSU	Network Service User
O&M	Operations & Maintenance
OMAP	Operations, Maintenance and Administration Part
OPC	Originating Point Code
OPT	Optional Field
OSI	Open Systems Interconnection
OSI-RM	OSI Reference Model
P(R)	Receive Sequence Number
P(S)	Send Sequence Number
PC	Point Code
PCI	Protocol Control Information
PCS	Personal Communications Service
PDU	Protocol Data Unit
PIN	Personal Identification Number

PLMN	Public Land Mobile Network
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAO	Regional Accounting Office
RIDB	Record Information Database
RLC	Release Complete
RLSD	Released
RSC	Reset Confirmation
RSR	Reset Request
SAAL	Signaling ATM Adaptation Layer
SBR	Subsystem-Backup-Routing
SC	Service Center
SCCP	Signaling Connection Control Part
SCLC	SCCP Connectionless Control
SCMG	SCCP Management
SCOC	SCCP Connection-Oriented Control
SCP	Service Control Point
SCRC	SCCP Routing Control
SDL	Specification and Description Language
SDU	Service Data Unit
SEP	Signaling End Point
SGSN	Serving GPRS Service Node
SIF	Signaling Information Field
SIO	Service Information Octet
SLS	Signaling Link Selection
SLS	Signaling Link Selection
SMDPP	Short Message Delivery Point To Point
SME	Short Message Entities
SMI	Subsystem Multiplicity Indicator
SMS	Short Message Services
SMS-PP	Short Message Service/Point-to-Point
SNR	Subsystem-Normal-Routing
SOG	Subsystem-Out-of-Service-Grant
SOR	Subsystem-Out-of-Service-Request
SPC	Signaling Point Code
SRT	Subsystem-Routing-Status-Test
SS7	Signaling System No. 7
SSA	Subsystem-Allowed
SSN	Subsystem Number
SSP	Subsystem-Prohibited
SSPN	Serving System Packet Node

SST	Subsystem-Status-Test
STP	Signaling Transfer Point
TC	Transaction Capabilities
TCAP	Transaction Capabilities Application Part
TI	Type Indicator
TIA	Telecommunications Industry Association
TLDN	Temporary Local Directory Number
TMSI	Temporary Mobile Station Identity
TT	Translation Type
UDT	Unitdata
UDTS	Unitdata Service
VLR	Visited Location Register
XUDT	Extended Unitdata
XUDTS	Extended Unitdata Service

NORMATIVE REFERENCES

The following standards contain provisions that, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

T1.110-1999 (R2005), *Signaling System No. 7 (SS7), General Information*.[1]

ATIS-1000111.2005, *Signaling System No. 7 (SS7), Message Transfer Part*.[1]

ATIS-1000113.2005, *Signaling System No. 7 (SS7) - Integrated Services Digital Network (ISDN) User Part*.[1]

ATIS-1000003, October 2004, *Number Portability Database and Global Title Translation.*[1]

ITU-T Recommendation E.164 (05/97), *The international public telecommunication numbering plan*.[2]

ITU-T Recommendation E.210 (11/88), *Ship station identification for VHF/UHF and maritime mobile-satellite services*.[2]

ITU-T Recommendation E.211, *Selection procedures for VHF/UHF maritime mobile services*.[2]

ITU-T Recommendation E.212 (05/04), *The international identification plan for mobile terminals and mobile users*.[2]

ITU-T Recommendation E.214 (02/05), *Structure of the land mobile global title for the signaling connection control part (SCCP)*.[2]

ITU-T Recommendation F.69 (06/94), *The international telex service - Service and operational provisions of telex destination codes and telex network identification codes*.[2]

ITU-T Recommendation X.121 (10/00), *International numbering plan for public data networks*.[2]

ITU-T Recommendation X.213 (10/01), *Information technology – Open Systems Interconnection – Network service definition.*[2]

---

[1] This document is available from the Alliance for Telecommunications Industry Solutions, 1200 G Street N.W., Suite 500, Washington, DC 20005. <http://www.atis.org>

[2] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

Chapter 1
Functional Description of the Signaling Connection Control Part

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

American National Standard for Telecommunications –

Functional Description of the Signaling Connection Control Part

1 SCOPE, PURPOSE, AND APPLICATION

1.1 General

The Signaling Connection Control Part (SCCP) provides additional functions to the Message Transfer Part (MTP) to provide both connectionless as well as connection-oriented network services to transfer circuit-related and non circuit-related signaling information and other types of information between exchanges and specialized centers in telecommunication networks (e.g., for management and maintenance purposes) via a Signaling System No. 7 (SS7) network.

A functional block situated above the MTP, (see T1.110-1999 (R2005)), performs the functions and procedures of the SCCP. The SCCP is capable of using the services of the MTP as described in ATIS-1000111, chapters ATIS-1000111.1 to ATIS-1000111.8. The combination of the MTP and the SCCP is called the Network Service Part (NSP).

1.2 Objectives

The overall objectives of the SCCP are to provide the means for:

1. Logical signaling connections within the Common Channel Signaling Network; and
2. A transfer capability for signaling data units with or without the use of logical signaling connections.

Functions of the SCCP are used for the transfer of circuit related and non circuit-related signaling information of the ISDN User Part with or without setup of end-to-end signaling connections. These functions are described in ATIS-1000112.4 and ATIS-1000113.4. Figure 1/ATIS-1000112.1 illustrates the embedding of the SCCP within the common-channel signaling system.

1.3 General Characteristic

1.3.1 Technique of Description

The SCCP is described in terms of:

1. Services provided by the SCCP.
2. Services assumed from the MTP.
3. Functions of the SCCP.

The functions of the SCCP are performed by means of the SCCP protocol between two systems which provide the SCCP service to the user located above the SCCP layer. The service interfaces to the upper layers and to the MTP are described by means of primitives and parameters. Figure 2/ATIS-1000112.1 illustrates the relationship between the SCCP protocol and the adjacent services.

1.3.2 Primitives

Primitives consist of commands and their respective responses associated with the services requested of the SCCP and of the MTP, see Figure 3/ATIS-1000112.1.

The general syntax of a primitive is shown below:

X	Generic Name	Specific Name	Parameters

1. "X" designates the functional block providing the service ("MTP" for MTP, "N" for SCCP)
2. "Generic Name" describes the action that should be performed by the addressed layer
3. "Specific Name" indicates the direction of the primitive flow
4. "Parameters" are the elements of information which are to be transmitted between layers.

Four Specific Names exist in general, see Figure 4/ATIS-1000112.1:

- Request
- Indication
- Response
- Confirm

Not all four Specific Names are associated with Generic Names (see Table 1/ATIS-1000112.1 and Table 8/ATIS-1000112.1).

1.3.3 Peer-to-Peer Communication

Exchange of information between two peers of the SCCP is performed by means of a protocol. The protocol is a set of rules and formats by which the control information (and user data) is exchanged between the two peers. The protocol provides for:

1. The setup of logical signaling connections
2. The release of logical signaling connections
3. The transfer of data with or without logical signaling connections.

A signaling connection is modeled in the abstract by a pair of queues. The protocol elements are objects on that queue added by the origination SCCP user and removed by the destination SCCP user. Each queue represents a flow control function. Figure 5/ATIS-1000112.1 illustrates the modes described above. (Model for the connectionless service is for further study.)

1.3.4 Contents of ATIS-1000112

Chapter 1 contains a general description of the services provided by the MTP, the services provided by the SCCP and the functions within the SCCP. Chapter 2 defines the set of protocol elements and their embedding into messages. Chapter 3 describes the formats and codes used for the SCCP messages. Chapter 4 is a detailed description of the SCCP procedures as a protocol specification. Chapter 5 provides the performance requirements for the SCCP. Chapter 6 provides the SCCP Users' Guide (Informative).

2 SERVICES PROVIDED BY THE SCCP

The overall set of services is grouped into:

1. Connection-oriented services; and
2. Connectionless services.

Four classes of services are provided by the SCCP protocol: two for connectionless services and two for connection-oriented services. The four classes are:

0 Basic connectionless class.

1 In-sequence delivery connectionless class.

2 Basic connection-oriented class.

3 Flow control connection-oriented class.

In the tables defining individual primitives, the notations given below are used:

M indicates a mandatory parameter;

O indicates an SCCP implementation option;

C indicates that the parameter is conditional;

U indicates a user option; and

= indicates the parameter must have the same value in the indication primitive, or confirm primitive as provided in the corresponding request primitive, or response primitive, respectively.

2.1 Connection-Oriented Services

A distinction has to be made between:

1. Temporary signaling connections; and
2. Permanent signaling connections.

Temporary signaling connection establishment is initiated and controlled by the SCCP user. Temporary signaling connections are comparable with dialed telephone connections.

Permanent signaling connections are established and released by Management and are provided to the SCCP user on a semi-permanent basis (comparable with leased telephone lines), while data including reset is under control of the SCCP user. Further details are given in clause 2.1.1.

2.1.1 Temporary Signaling Connections

2.1.1.1 Description

The control of a signaling connection is divided into the following phases:

1. Connection establishment phase
2. Data transfer phase
3. Connection release phase.

2.1.1.1.1 Connection Establishment Phase

Connection establishment procedures provide the mechanism for establishing temporary signaling connections between users of the SCCP.

A signaling connection between two SCCP users may consist of one or more connection sections. A signaling connection between two SCCP users in the same node is considered an implementation dependant matter.

During connection establishment, routing functions are provided by the SCCP, in addition to those provided by the MTP.

At intermediate nodes, SCCP routing determines whether a signaling connection should be realized by one connection section or several concatenated connection sections. The criteria for deciding on several concatenated connection sections are implementation dependant.

For Connection establishment there are two alternative boundaries between SCCP and SCCP user with different procedures;

- ♦ The "X.213-like" boundary that is described further in clause 2.1.1.2; and
- ♦ The "ISUP-embedded" boundary that is described further in clause 2.1.1.3.

The "X.213-like" boundary requires that establishment procedures are performed by SCCP while in the case of "ISUP-embedded" boundary the ISUP provides the routing of the request for the set-up of a connection section.

The connection refusal procedure is invoked if the SCCP or the SCCP user is unable to establish a signaling connection.

2.1.1.1.2 Data Transfer Phase

The data transfer service provides for an exchange of user data, called Network Service Data Units (NSDU), in either direction or in both directions simultaneously on a signaling connection. Each NSDU is characterized by a connection identification which allocates the message to a certain signaling connection. The data transfer service provides for segmenting of messages, concatenation of messages, flow control, error detection, sequence control, and other functions, depending on the quality of service required by the SCCP user (two different classes of the connection-oriented service are provided by the protocol, see ATIS-1000112.4).

2.1.1.1.3 Connection Release Phase

Connection release procedures provide the mechanism for releasing temporary signaling connections between users of the SCCP. The signaling connection may be released by both or either of the SCCP users. The signaling connection may also be released by the SCCP if the connection can not be maintained.

2.1.1.2 Network Service Primitives and Parameters Applicable To The X.213-Like Connection-Oriented Boundary

2.1.1.2.1 Overview

Table 1/ATIS-1000112.1 gives an overview of the primitives to the upper layers and the corresponding parameters for the (temporary) connection-oriented network service. Figure 6/ATIS-1000112.1 shows an overview state transition diagram for the sequence of primitives at a connection endpoint.

A more detailed description for the primitives and their parameters is given in the following chapters.

2.1.1.2.2 Connection Establishment Phase

A network service user (calling user) initiates the setup of the connection by means of the primitive "N-CONNECT request" to the SCCP. The SCCP entity evaluates the primitive and adds the protocol control information. The SCCP message -- consisting of the protocol control information (PCI) and possibly an NSDU -- is transmitted by means of the MTP-services to the remote peer entity of the SCCP. It evaluates and strips the PCI, and sends a primitive "N-CONNECT indication" to the local network service user. On both ends of the connection the status "pending" is assumed.

The called SCCP user answers with the primitive "N-CONNECT response" to the local SCCP, which sends the response SCCP message, including PCI, to the calling SCCP. The calling SCCP sends the primitive "N-CONNECT confirm" to the calling SCCP user. The connection is now ready for data transfer.

The four types of N-CONNECT applicable to the X.213-like boundary, the "request," the "indication," the "response," and the "confirm," contain the parameters as shown and further described in Table 2/ATIS-1000112.1.

The parameters "called address" and "calling address" convey addresses identifying the destination/source of a communication. There are three types of addresses:

1. Global Title;
2. Subsystem Number; and
3. Signaling Point Code.

The Global Title is an address such as dialed digits which does not explicitly contain information that would allow routing in the signaling network (i.e., a translation function is required). The Subsystem Number is an identification of a specific user function within a certain Signaling Point like the ISDN-User Part, the SCCP-Management, etc. The parameter "responding address" indicates to which destination the connection has been established or refused.

The Responding Address parameter in the N-CONNECT confirm primitive conveys the address of the service access point to which the signaling connection has been established. Under certain circumstances (e.g., call redirection, generic addressing), the value of this parameter may be different from the called address in the corresponding N-CONNECT request.

The Responding Address parameter is present in the N-DISCONNECT primitive only in the case where the primitive is used to indicate rejection of a signaling connection establishment attempt by an SCCP user function. This parameter conveys the address of the service access point from which the N-DISCONNECT request was issued, and under circumstances like that mentioned above, the Responding Address may be different from the Called Address in the corresponding N-CONNECT request primitive.

The parameter "expedited data selection" may be used to indicate during setup whether expedited data can be transferred via the connection. A negotiation will be performed between SCCP users, local and remote.

The quality of service parameters are used during call setup to negotiate the protocol class for the connection and, if applicable, the flow control window size.

The N-CONNECT primitives may or may not contain user data.

The parameter "connection identification" is used to allocate a primitive to a certain connection. The connection identification is internal representation of the "connection end point identifier" defined in the OSI-RM. Its use and format is implementation dependent.

In principle, the connection establishment has to be completed (i.e., data transfer status has to be reached) before sending or receiving data messages. If data messages arrive at the calling user before the connection establishment is finished, these data messages are discarded.

In addition, user data can also be transferred to/from the SCCP within the primitives N-CONNECT and N-DISCONNECT.

2.1.1.2.3 Data Transfer Phase

During this phase, three different primitives may occur:

1. N-DATA (Table 3/ATIS-1000112.1)
2. N-EXPEDITED DATA (Table 4/ATIS-1000112.1)
3. N-RESET (Table 5/ATIS-1000112.1)

The primitive "N-DATA" exists only as a "request" (i.e., from the SCCP user to the local SCCP) and as an "indication" at the remote end of the connection (i.e., from the SCCP to the local SCCP user). N-DATA can occur bi-directionally (i.e., from the calling to called user or the called to calling user of the SCCP-connection).

The primitive "N-EXPEDITED DATA" may only be used by the SCCP user in case of protocol class 3 connections.

The primitive "N-RESET" (Table 5/ATIS-1000112.1) can occur in the data transfer state of a connection with a protocol class including flow control. N-RESET overrides all other activities and causes the SCCP to start a re-initialization procedure for sequence numbering. N-RESET appears as a "request," an "indication," a "response," and a "confirm." After reception of an N-RESET request and before the sending of an N-RESET confirm, all NSDUs are discarded.

The parameter "originator" indicates the source of the reset and can be any of the following: the "network service provider" (network originated), the "network service user" (user originated), or "undefined." The parameter "reason" indicates "network service provider congestion" or "reason unspecified" for a user originated reset. The "reason" parameter is "undefined" when the "originator" parameter is "undefined."

2.1.1.2.4 Release Phase

The primitives for the release phase are "N-DISCONNECT request" and "N-DISCONNECT indication." These primitives are also used for the connection refusal during the connection establishment phase. Parameters are included to notify the reason for connection release/refusal and the initiator of the connection release/refusal procedure. User data may be added (see Table 6/ATIS-1000112.1).

The parameter "originator" indicates the initiator of the connection release or the connection refusal. It may assume the following values:

1. The network service provider
2. The network service user
3. Undefined

The parameter "reason" gives information about the cause of the connection release or the connection refusal. It may assume any of the following values in accordance with the value of the "originator":

1. When the "originator" parameter indicates the "network service provider":
    a. Disconnection – abnormal condition of non-transient nature[1]
    b. Disconnection – abnormal condition of transient nature
    c. Disconnection – invalid state[1]
    d. Disconnection – release in progress[1]
    e. Connection refusal - destination address unknown (non-transient condition)
    f. Connection refusal - destination inaccessible/non-transient condition[1]
    g. Connection refusal - destination inaccessible/transient condition
    h. Connection refusal - QOS not available/non-transient condition
    i. Connection refusal - QOS not available/transient condition
    j. Connection refusal - reason unspecified/non-transient condition
    k. Connection refusal - reason unspecified/transient condition
    l. Connection refusal - local error[1]
    m. Connection refusal - invalid state[1]

[1] These values may be used locally at the originating/initiating node as an implementation option.

n. Connection refusal - no translation[1]

o. Connection refusal - in restart phase[1]

p. Connection refusal - hop counter violation

2. When the "originator" parameter indicates the "network service user":

    a. Disconnection – normal condition
    b. Disconnection – abnormal condition
    c. Disconnection - end user congestion
    d. Disconnection - end user failure
    e. Disconnection – SCCP user originated
    f. Disconnection - access congestion
    g. Disconnection - access failure
    h. Disconnection - subsystem congestion
    i. Connection refusal - non-transient condition
    j. Connection refusal - transient condition
    k. Connection refusal - incompatible information in NSDUs
    l. Connection refusal - end user originated
    m. Connection refusal - end user congestion
    n. Connection refusal - end user failure
    o. Connection refusal - SCCP user originated
    p. Connection refusal - access congestion
    q. Connection refusal - subsystem congestion

3. When the "originator" parameter is "undefined", then the "reason" parameter is also "undefined".

2.1.1.2.5 Notice Service

The primitive N-INFORM (Table 6A/ATIS-1000112.1) is used during data transfer to convey relevant network/user information. The primitive N-INFORM will contain the parameters "reason," "connection identification," and "quality of service (QOS) parameter set."

The primitive "N-INFORM request" is provided to inform the SCCP of the connection user failure/congestion, or anticipated QOS changes. A further primitive "N-INFORM indication" is provided to indicate actual failures of the SCCP to the SCCP user functions or anticipated QOS changes or other indications to the SCCP user functions.

The parameter "reason" contains the network/user information to be conveyed. It may assume the following values:

1. Network service provider failure
2. Network service provider congestion
3. Network service provider QOS change

4. Network service user failure
5. Network service user congestion
6. Network service user QOS change
7. Unspecified

2.1.1.3 Network Service Primitives, Interface Elements And Parameters Applicable To The ISUP-Embedded Connection-Oriented Boundary

2.1.1.3.1 Overview

Table 6B/ATIS-1000112.1 gives an overview of the primitives to the SCCP user layer and the corresponding parameters for the (temporary) "ISUP-embedded" connection-oriented network service. The state transition diagram for the sequences of the primitives at a connection endpoint is left for further study.

2.1.1.3.2 Connection establishment making use of the ISUP-embedded procedures

An SCCP user (calling user) may, instead of using the N-CONNECT.request thereby requesting SCCP to transmit appropriate Protocol Data Unit (PDU), use the REQUEST to solicit the SCCP to provide in the REPLY information relevant for connection establishment. The forward direction of the connection is established hop-by-hop making use of PDUs of ISUP thereby is embedded in the forward call set-up. In the backward direction, normal SCCP PDUs are used. The N-CONNECT.request is replaced at the origin by the two interface elements REQUEST type 1 and REPLY. Within intermediate nodes the two interface elements REQUEST type 2 and REPLY are required.

The three types of N-CONNECT applicable to the ISUP embedded boundary, the indication, the response, and the confirm contain the parameters as shown in Table 6C/ATIS-1000112.1.

Three interface elements are defined for the information flow between the SCCP and ISDN-User Part:

1. REQUEST to the SCCP, Type 1
2. REQUEST to the SCCP, Type 2
3. REPLY from the SCCP

The REQUEST Type 1, which requests connection establishment information for an outgoing connection section from the SCCP originating node, contains the following parameters:

1. Connection identification (O)
2. Expedited data selection (U)
3. Quality of service parameter set (U)

REQUEST type 2, contains the following parameters:

1. Quality of service parameter set (U)
2. Connection identification (O)
3. Source local reference (M)
4. Originating Signaling Point Code (M)

5. Reply request (U)
6. Refusal indicator (U)

The REPLY contains the following parameters:

1. Source Local reference (M)
2. Quality of service parameter set (M)
3. Connection identification (O)

2.1.2 Permanent Signaling Connections

2.1.2.1 Description

The setup/release service is controlled by the Administration (e.g., O&M application). The functions for setup and release may be similar to those provided for temporary signaling connections. The classes of service are the same.

Permanently established signaling connections may require additional safeguarding mechanisms within the endpoints (relay points) of the connection in order to guarantee their re-establishment in the case of a processor outage followed by a recovery.

2.1.2.2 Primitives and Parameters

The primitives and their parameters are listed in Table 7/ATIS-1000112.1. Their content and functionality correspond to the description within clause 2.1.1.2.3.

2.2 Connectionless Service

The SCCP provides the SCCP user with the ability to transfer signaling messages via the signaling network without setup of a signaling connection. In addition to the MTP-capability, a "Routing" function is provided within the SCCP which maps the called address (and any optional routing parameters) to the Signaling Point Codes of the MTP-Service. This mapping function may be provided within each node or might be distributed over the network or could be provided in some special translation centers. Under certain conditions (e.g., congestion and unavailability of subsystems and/or signaling points), connectionless messages could be discarded instead of being delivered. If the SCCP user wishes to be informed of the non-delivery of messages, the parameter "Return Option" must be set to "return message on error" in the primitive to the SCCP.

2.2.1 Description

There are two possibilities to transfer data without a connection setup with regard to the sequence control mechanisms provided by the MTP.

The MTP guarantees (to a high degree of probability) an in-sequence delivery of messages which contain the same Signaling Link Selection (SLS) code. The SCCP user can demand this MTP-service by allocating a parameter "sequence control" into the primitive to the SCCP. The SCCP will put the same

SLS code into the primitive to the MTP for all primitives from the SCCP user with the same sequence control parameter.

If the in-sequence delivery is not required, the SCCP can insert SLS codes randomly or with respect to appropriate load sharing within the signaling network.

2.2.2 Primitives and Parameters of the Connectionless Service

2.2.2.1 Overview

Table 8/ATIS-1000112.1 gives an overview of the primitives to the upper layers and the corresponding parameters for the connectionless service.

2.2.2.2 Parameters

2.2.2.2.1 Address

The parameters "called address" and "calling address" serve to identify the destination and origination respectively, of the connectionless message. These parameters may contain some combination global titles, subsystem numbers, and signaling point codes.

2.2.2.2.2 Quality of service parameter set

The quality of service parameter set contains the following parameters: sequence control, return option, and message priority.

1. *Sequence Control*. The parameter "sequence control" indicates to the SCCP whether the user wishes the service "sequence guaranteed" or the service "sequence not guaranteed." In the case of sequence guaranteed service, this parameter is an indication to the SCCP that a given stream of messages with the same called address has to be delivered in sequence by making use of the features of the MTP. In addition, this parameter is also used to distinguish between different streams of messages such that an even distribution of SLS codes will result.
2. *Return Option*. The parameter "return option" is used to determine the handling of messages encountering transport problems. "Return option" may assume the following values:
    a. Discard message on error.
    b. Return message on error.
3. *Message Priority*. The general message priority guidelines and the priority assignments for SCCP messages are provided in ATIS-1000111.5, Annex B, clause B.3, and Table 4, respectively.

2.2.2.2.3 Reason for Return

The parameter "reason for return" identifies the reason why a message was not able to be delivered to its final destination. See ATIS-1000112.3, clause 3.12, Return cause (formerly Diagnostic), for the values that may be assumed.

2.2.2.2.4 User Data

The parameter "user data" contains information that is to be transferred transparently between SCCP users.

2.2.2.3 Primitives

2.2.2.3.1 N-UNITDATA

The "N-UNITDATA request" primitive is the means by which an SCCP user requests the SCCP to transport data to a peer SCCP user. The "N-UNITDATA indication" primitive informs a user that data is being delivered to it from the SCCP (See Table 8A/ATIS-1000112.1).

2.2.2.3.2 N-NOTICE

The "N-NOTICE indication" primitive is the means by which the SCCP returns to the originating user a message which could not reach the final destination (See Table 8B/ATIS-1000112.1).

2.3 SCCP Management

2.3.1 Description

The SCCP provides SCCP management procedures to maintain network performances by rerouting or throttling traffic in the event of failure or congestion in the network. These SCCP management procedures apply to both the connection-oriented and the connectionless services of the SCCP.

2.3.2 Primitives and Parameters of the SCCP Management

2.3.2.1 Overview

Table 8C/ATIS-1000112.1 gives an overview of the primitives to the upper layers and the corresponding parameters for the SCCP management.

2.3.2.2 Parameters

2.3.2.2.1 Address

See clause 2.2.2.2.1.

2.3.2.2.2 Affected User

The parameter "affected user" identifies an affected user that is failed, withdrawn (or has requested withdrawal), congested, or allowed. The affected user parameter contains the same type of information as the called address and calling address. In the case of the N-TRAFFIC primitive (see clause 2.3.2.3.3), the parameter identifies the user from which a preferred subsystem is receiving backup traffic.

2.3.2.2.3 User Status

The parameter "user status" is used to inform an SCCP user of the status of the affected user. "User status" may assume one of the following values:

1. User in-service.
2. User out-of-service.

2.3.2.2.3A Traffic Mix

The optional parameter "traffic mix" is used to inform an SCCP user what traffic pattern it is receiving. Traffic mix may assume the following values:

1. All-preferred/No-backup.
2. All-preferred/Some-backup.
3. All-preferred/All-backup.
4. Some-preferred/No-backup.
5. Some-preferred/Some-backup.
6. No-preferred/No-backup.
7. All.
8. Some.
9. None.

2.3.2.2.4 Subsystem Multiplicity Indicator

The parameter "subsystem multiplicity indicator" identifies the number of replications of a subsystem. Subsystem multiplicity indicator may assume the following values:

1. Replicated.
2. Solitary.
3. Unknown.

2.3.2.2.5 Affected DPC

The parameter "affected DPC" identifies a signaling point which is failed, congested, or allowed. The "affected DPC" parameter contains unique identification of a signaling point.

2.3.2.2.6 Signaling Point Status

The parameter "signaling point status" is used to inform a user of the status of an affected DPC. Signaling point status may assume the following values:

1. Signaling point inaccessible.
2. Signaling point congested.
3. Signaling point accessible.

2.3.2.2.7 Confirm Status

The parameter "confirm status" is used to inform an SCCP user whether the user out-of-service request is granted or denied. "Confirm status" may assume the following values:

1. User out-of-service request granted.
2. User out-of-service request denied.

2.3.2.3 Primitives

2.3.2.3.1 N-COORD

The "N-COORD" primitive is used by replicated subsystems to coordinate the withdrawal of one of the subsystems. The primitive exists as: a "request" when the originating user is requesting permission to go out of service; an "indication" when the request to go out of service is delivered to the originator's replicate; a "response" when the originator's replicate announces it has sufficient resources to let the originator go out of service; and as a "confirm" when the originator is informed that it may or may not go out of service (See Table 8D/ATIS-1000112.1).

2.3.2.3.2 N-STATE

The "N-STATE request" primitive is used to inform SCCP Management about the status of the originating user. The "N-STATE indication" primitive is used to inform a user about the status of the affected user (See Table 8E/ATIS-1000112.1).

2.3.2.3.3 N-TRAFFIC

The "N-TRAFFIC indication" primitive is used to inform a local user what traffic pattern it is receiving (See Table 8F/ATIS-1000112.1).

2.3.2.3.4 N-PCSTATE

The "N-PCSTATE" primitive is used to inform a user about the status of a signaling point (See Table 8G/ATIS-1000112.1).

3 SERVICES ASSUMED FROM THE MTP

3.1 Description

This clause describes the functional interface offered by the MTP to the upper layer functions (i.e., the SCCP and the User Parts). In order to align the terminology with the OSI Model, the description uses the terms "primitives" and "parameters."

The services provided by the MTP can be offered by two different MTP networks depending on the capability of the link level protocol (see ATIS-1000111.1):

1. An MTP network that supports a maximum MTP-SDU size of 272 octets, including the MTP routing label (see ATIS-1000111.3).
2. An MTP network that supports a maximum MTP-SDU size of 4095 octets, including MTP routing label (see ATIS-1000111.3).

With the exception of the maximum supported SDU size, these two MTP networks offer equivalent services.

3.2 Primitives and Parameters

The primitives supported by the MTP are specified in Table 1/ATIS-1000111.1. Table 9/ATIS-1000112.1 specifies how the MTP-primitives apply when SCCP is using the services of the MTP. In the case of conflicting statements between ATIS-1000112.1 and ATIS-1000111.1, ATIS-1000111.1 takes precedence.

3.2.1 MTP-TRANSFER

The primitive "MTP-TRANSFER" is used between level 4 and level 3 (Signaling Message Handling) for message transfer service provided by the MTP.

3.2.2 MTP-PAUSE

The primitive "MTP-PAUSE" is an indication from the MTP to the SCCP of the total inability of providing the MTP service to the specified destination. The primitive corresponds to the destination inaccessible state as defined in ATIS-1000111.4.

3.2.3 MTP-RESUME

The primitive "MTP-RESUME" is an indication from the MTP to the SCCP of the total ability of providing the MTP service to the specified destination. This primitive corresponds to the destination accessible state as defined in ATIS-1000111.4.

3.2.4 MTP-STATUS

The primitive "MTP-STATUS" is an indication from the MTP to the SCCP of the partial inability of providing the MTP service to the specified destination. The "MTP-STATUS" primitive is also used to indicate a change in congestion level. This primitive corresponds to the destination congested state as defined in ATIS-1000111.4.

4 FUNCTIONS PROVIDED BY THE SCCP

4.1 Connection-Oriented Functions

This clause is an overview of the functional blocks within the SCCP.

4.1.1 Functions for Temporary Signaling Connections

4.1.1.1 Connection Establishment Functions

The connection establishment service primitives defined in clause 2 are used to set up a signaling connection. The main functions of the connection establishment phase are listed below:

1. Setup of a signaling connection.
2. Establish the optimum size of NPDUs (Network Protocol Data Unit).
3. Map network address onto signaling relations.
4. Select functions operational during data transfer phase (e.g., class of service).
5. Provide means to distinguish network connections.
6. Transport user data (within the request).

4.1.1.2 Data Transfer Phase Functions

The data transfer phase functions provide means for a two-way simultaneous transport of messages between the two endpoints of the signaling connection. The main functions of the data transfer phase as listed below are used or not used in accordance with the result of the selection performed in the connection phase:

1. Segmenting/Reassembling.
2. Flow Control.
3. Connection Identification.
4. NSDU Delimiting (M-Bit).
5. Expedited Data.
6. Missequence Detection.
7. Reset.
8. Other.

4.1.1.3 Release Phase Functions

These functions provide disconnection of the signaling connection, regardless of the current phase of the connection. The release may be performed by an upper layer stimulus or by maintenance of the SCCP itself. The release can start at each end of the connection (symmetrical procedure). The main function of the release phase is the disconnection.

4.1.2 Functions for Permanent Signaling Connections

4.1.2.1 Connection Establishment Phase and Connection Release Phase Functions

The stimuli for setup and release of permanent connections are originated from the Administration function.

4.1.2.2 Data Transfer Phase Functions

The functions for the data transfer on permanent signaling connections correspond to those for temporary connections. Differences will exist regarding the quality of service and the classification of services.

4.2 Connectionless Service Functions

The functions of the connectionless service are listed below:

1. Mapping the network address to signaling relations (see clause 2.2).
2. Segmenting.
3. Sequence service classification (see clause 2.2.1).

Table 1/ATIS-1000112.1 - Network Service Primitives for X.213-like Connection-Oriented Services

Primitives		**Parameters**
Generic Name	Specific Name	
N-CONNECT	Request Indication Response Confirm	See Table 2/ATIS-1000112.1
N-DISCONNECT	Request Indication	Originator Responding address Reason User data Connection identification
N-DATA	Request Indication	User data Connection identification
N-EXPEDITED DATA	Request Indication	User Data Connection Identification
N-RESET	Request Indication Response Confirm	Originator Reason Connection Identification[2]
N-INFORM[a]	Request Indication	Reason Source local ref. QOS parameter set[a]

a) This primitive is not in Recommendation X.213.

[2] In 5.3/X.213, this parameter is implicit.

Table 2/ATIS-1000112.1 - Parameters of the Primitive N-CONNECT

Parameter	Primitive			
	N-CONNECT Request	N-CONNECT Indication	N-CONNECT Response	N-CONNECT Confirm
Called address	M	M[a2]		
Calling address	U[a1]	C[c1]		
Responding address			U[a3]	C[c1]
Expedited data selection	U		U	
Quality of service parameter set	M	M	M	M(=)
User data	U	C(=)[c1]	U	C(=)[c1]
Connection Identification	O	O	O	O

[a1] This parameter is associated with the SCCP service access point at which this primitive is issues if the called address is absent.

[a2] This parameter is associated with the SCCP service access point at which this primitive is issued if the called address is absent.

[a3] This parameter is associated with the SCCP service access point at which this primitive is issued if the responding address is absent.

[c1] If present in the received message.

Table 3/ATIS-1000112.1 - Parameters of the Primitive N-DATA

Parameter	Primitive	
	N-DATA Request	N-DATA Indication
User Data	M	M(=)
Connection Identification	O	O

Table 4/ATIS-1000112.1 - Parameters of the Primitive N-EXPEDITED DATA

Parameter	Primitive	
	N-EXPEDITED DATA Request	N-EXPEDITED DATA Indication
User data	M	M(=)
Connection Identification	O	O

Table 5/ATIS-1000112.1 - Parameters of the Primitive N-RESET

Parameter	Primitive			
	N-RESET Request	N-RESET Indication	N-RESET Response	N-RESET Confirm
Originator	(Always NSU)	M		
Reason	M	M		
Connection Identification	O	O	O	O

Table 6/ATIS-1000112.1 - Parameters of the Primitive N-DISCONNECT

Parameter	Primitive	
	N-DISCONNECT Request	N-DISCONNECT Indication
Originator	(Always NSU)	M
Responding address	U[a]	C[c2,a]
Reason	M	M
User data	U	C(=)[c2]
Connection Identification	O	O

[a] Only applicable in the case of connection refusal.

[c2] If present in the received SCCP message.

Table 6A/ATIS-1000112.1 - Parameters of the Primitive N-INFORM

Parameter	Primitive	
	N-INFORM Request	N-INFORM Indication
Reason	M	M
Connection Identification	O	O
QOS parameter set	C[c3]	C[c3]

[c3] Present in inform reasons that lead to a QOS parameter set change.

Table 6B/ATIS-1000112.1 - Network Service Primitives And Interface Elements For ISUP-Embedded Connection-Oriented Services

Generic Name		Parameters
Generic Name	Specific Name	
N-CONNECT	Indication Response Confirm	See Table 6C/ATIS-1000112.1
N-DISCONNECT	Request Indication	Originator Responding address Reason User data Connection identification[a]
N-DATA	Request Indication	User data Connection identification[a]
N-EXPEDITED DATA	Request Indication	User Data Connection Identification[a]
N-RESET	Request Indication Response Confirm	Originator Reason Destination local ref[a]. Source local ref[a].
N-INFORM[b]	Indication Request	Reason Source local ref. [a] QOS parameter set[b]
REQUEST type 1 - Connection identification[a] Expedited data selection QOS parameter set[b] REQUEST type 2 - QOS parameter set[b] Connection identification[a] Source local reference Originating Signaling Point Code Reply request REPLY - Source local reference QOS parameter set[b] Connection identification[a]		

[a] In X.213, clause 5.3, this parameter is implicit.
[b] This primitive is not in Recommendation X.213.

Table 6C/ATIS-1000112.1 - Parameters of the Primitive N-CONNECT

Parameter	Primitive		
	N-CONNECT Indication	N-CONNECT Response	N-CONNECT Confirm
Called address	O		
Calling address			
Responding address		U[a1]	C[c1]
Expedited data selection		U	
Quality of service parameter set	O	M	M(=)
User data		U	C(=)[c1]
Destination local reference	O	O	O
Source local reference	O	O	O

[a1] This parameter is associated with the SCCP service access point at which this primitive is issued if the called address is absent.

[c1] If present in the received message.

Table 7/ATIS-1000112.1 - Primitives for the Data Transfer on Permanent Connections

Primitives		Parameters
Generic Name	Specific Name	
N-DATA	Request Indication	User data Connection identification
N-EXPEDITED DATA	Request Indication	User data Connection identification
N-RESET	Request Indication Response Confirm	Originator Reason Connection identification

Table 8/ATIS-1000112.1 - Primitives and Parameters of the Connectionless Service

Primitives		Parameters
Generic Name	Specific Name	
N-UNITDATA	Request Indication	Called address Calling address Quality of service parameter set[a] User data
N-NOTICE	Indication	Called address Calling address Reason for return User data

[a] Contains sequence control, return option and message priority.

Table 8A/ATIS-1000112.1 - Parameters of the Primitive N-UNITDATA

Parameter	Primitive	
	N-UNITDATA Request	N-UNITDATA Indication
Called address	M	M
Calling address	U[a]	M
Quality of service parameter set	U	O
User data	M	M(=)
Optional parameters[b]	O	O

[a] This parameter is associated with the SCCP service access point at which the primitive is issued if the calling address is absent.

[b] Only allowed with LUDT, LUDTS, XUDT, and XUDTS messages.

Table 8B/ATIS-1000112.1 - Parameters of the Primitive N-NOTICE

Parameter	Primitive (N-NOTICE Indication)
Called address	M
Calling address	M
Reason for return	M
User data	M
Optional parameters	O

Table 8C/ATIS-1000112.1 - Primitives and Parameters of the SCCP Management

Primitives		Parameters
Generic name	Specific name	
N-COORD	Request Indication Response Confirm	Affected user Confirm status Subsystem multiplicity indicator
N-STATE	Request Indication	Affected user User status Subsystem multiplicity indicator
N-PCSTATE	Indication	Affected DPC Signaling point status
N-TRAFFIC	Indication	Affected user Traffic mix

Table 8D/ATIS-1000112.1 - Parameters of the Primitive N-COORD

Parameter	Primitive			
	N-COORD Request	N-COORD Indication	N-COORD Response	N-COORD Confirm
Affected user	M	M	M	M
Confirm status				M
Subsystem multiplicity indicator		O		O

Table 8E/ATIS-1000112.1 - Parameters of the Primitive N-STATE

Parameter	Primitive	
	N-STATE Request	N-STATE Indication
Affected user	M	M
User status	M	M
Subsystem multiplicity indicator	-	O

Table 8F/ATIS-1000112.1 - Parameters of the Primitive N-TRAFFIC

Parameter	Primitive (N-TRAFFIC Indication)
Affected user	M
Traffic mix	M

Table 8G/ATIS-1000112.1 - Parameters of the Primitive N-PCSTATE

Parameter	Primitive (N-PCSTATE Indication)
Affected DPC	M
Signaling point status	M

Table 9/ATIS-1000112.1 - Message Transfer Part Service Primitives

Primitives		Parameters
Generic name	Specific name	
MTP-TRANSFER	Request Indication	OPC DPC SLS SIO User data
MTP-PAUSE (Stop)	Indication	Affected DPC
MTP-RESUME (Start)	Indication	Affected DPC
MTP-STATUS	Indication	Affected DPC Cause

EDITORIAL NOTE - The standard numbering has changed in this version of ATIS-1000111, ATIS-1000112, and ATIS-1000113. These standards were formerly numbered as T1.111, T1.112, and T1.113 respectively. The associated chapter numbering has not been modified.

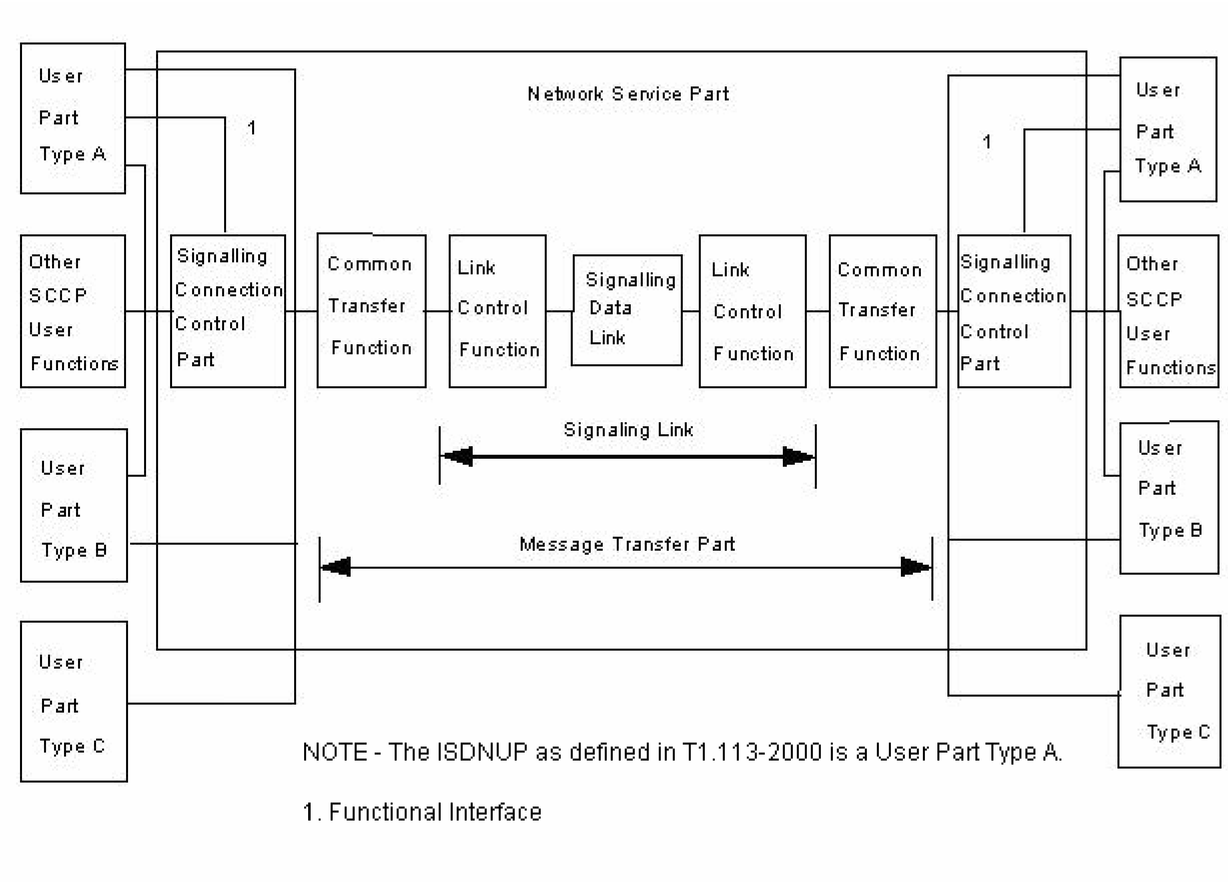


Figure 1/ATIS-1000112.1 - Functional Diagram for the Common Channel Signaling System

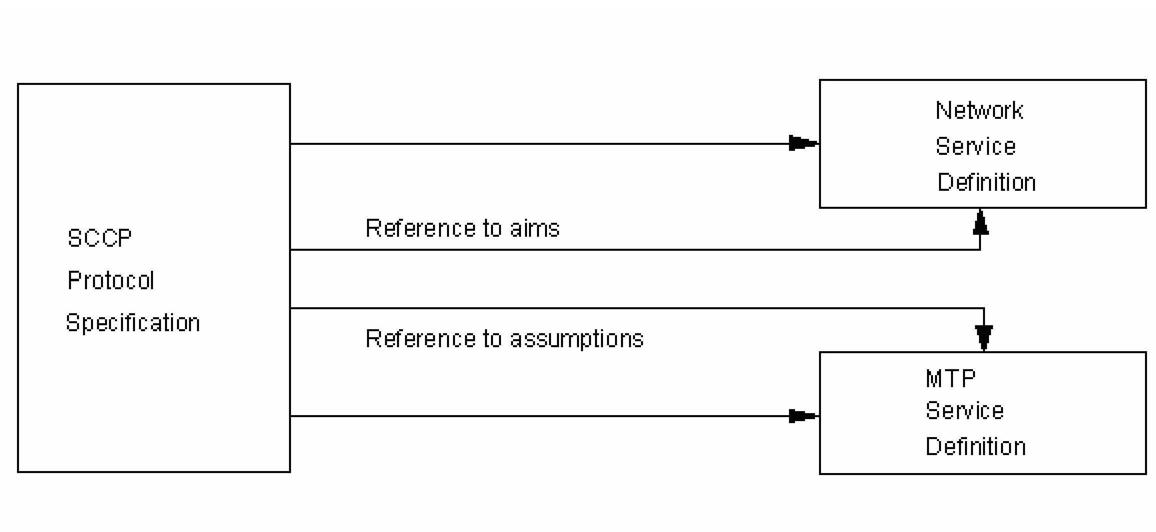


Figure 2/ATIS-1000112.1 - Relationship between the SCCP Protocol and Adjacent Services

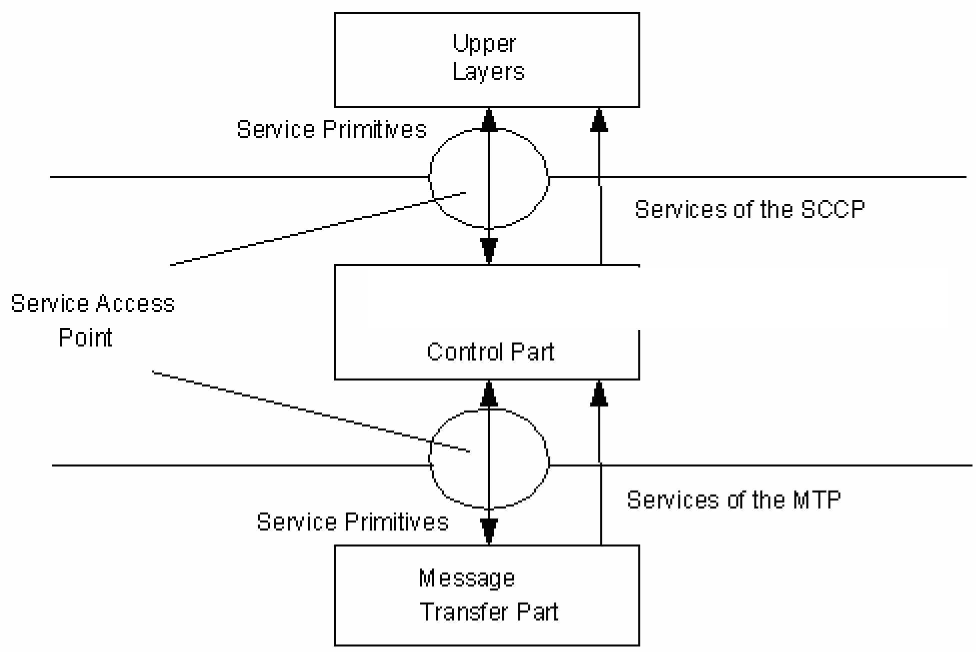


Figure 3/ATIS-1000112.1 - Service Primitives

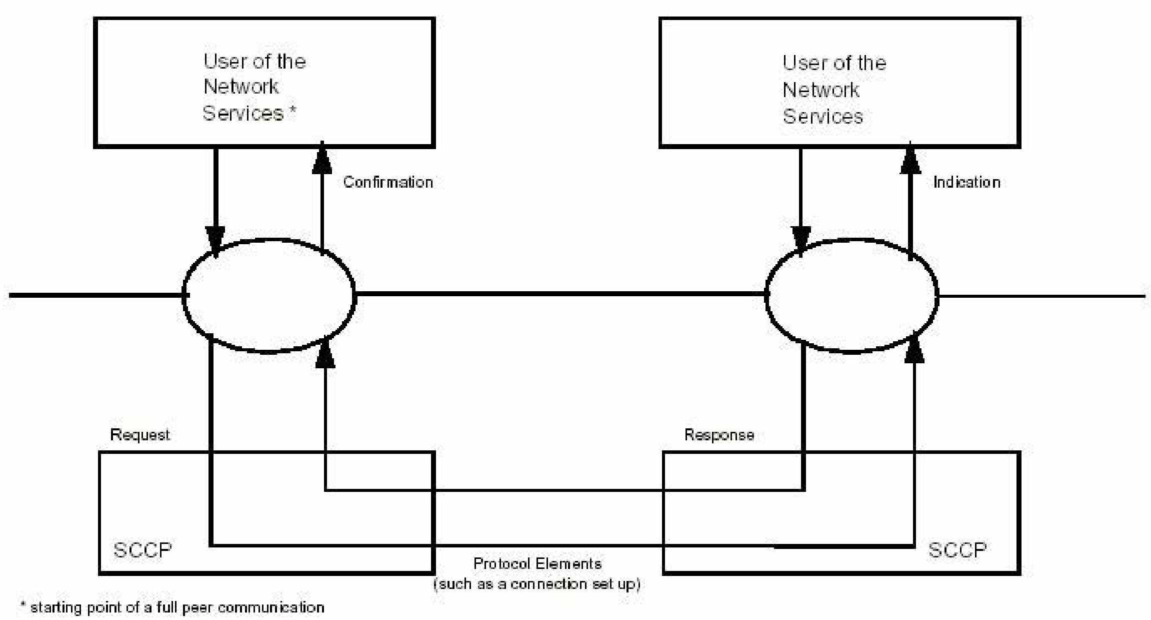


Figure 4/ATIS-1000112.1 - Specific Names of Service Primitives and Peer-to-Peer Communication

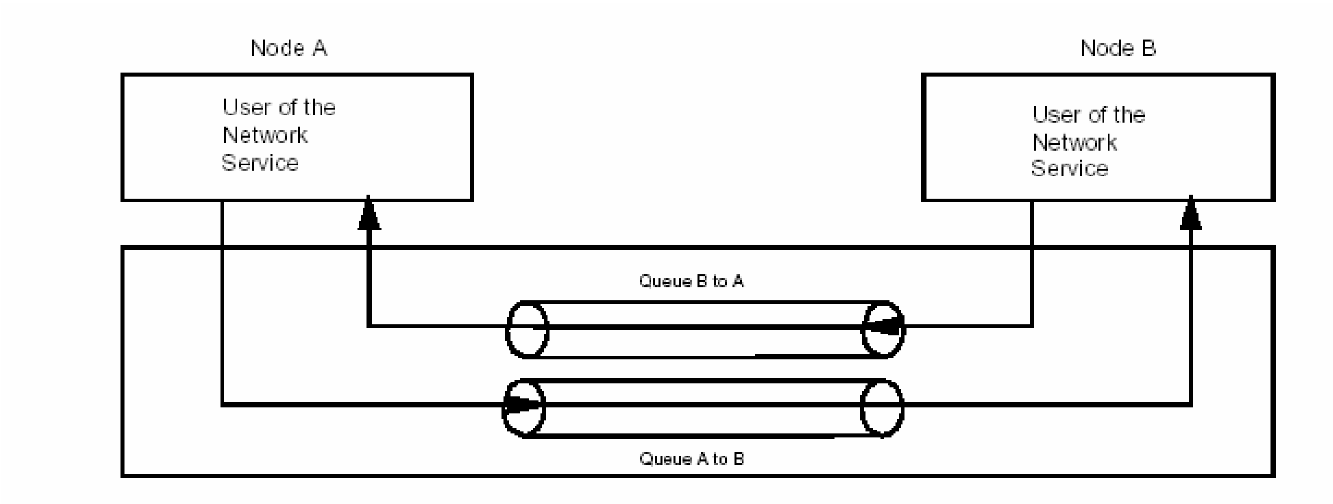


Figure 5/ATIS-1000112.1 - Model for the Internode Communication within the SCCP (Connection-Oriented Service)

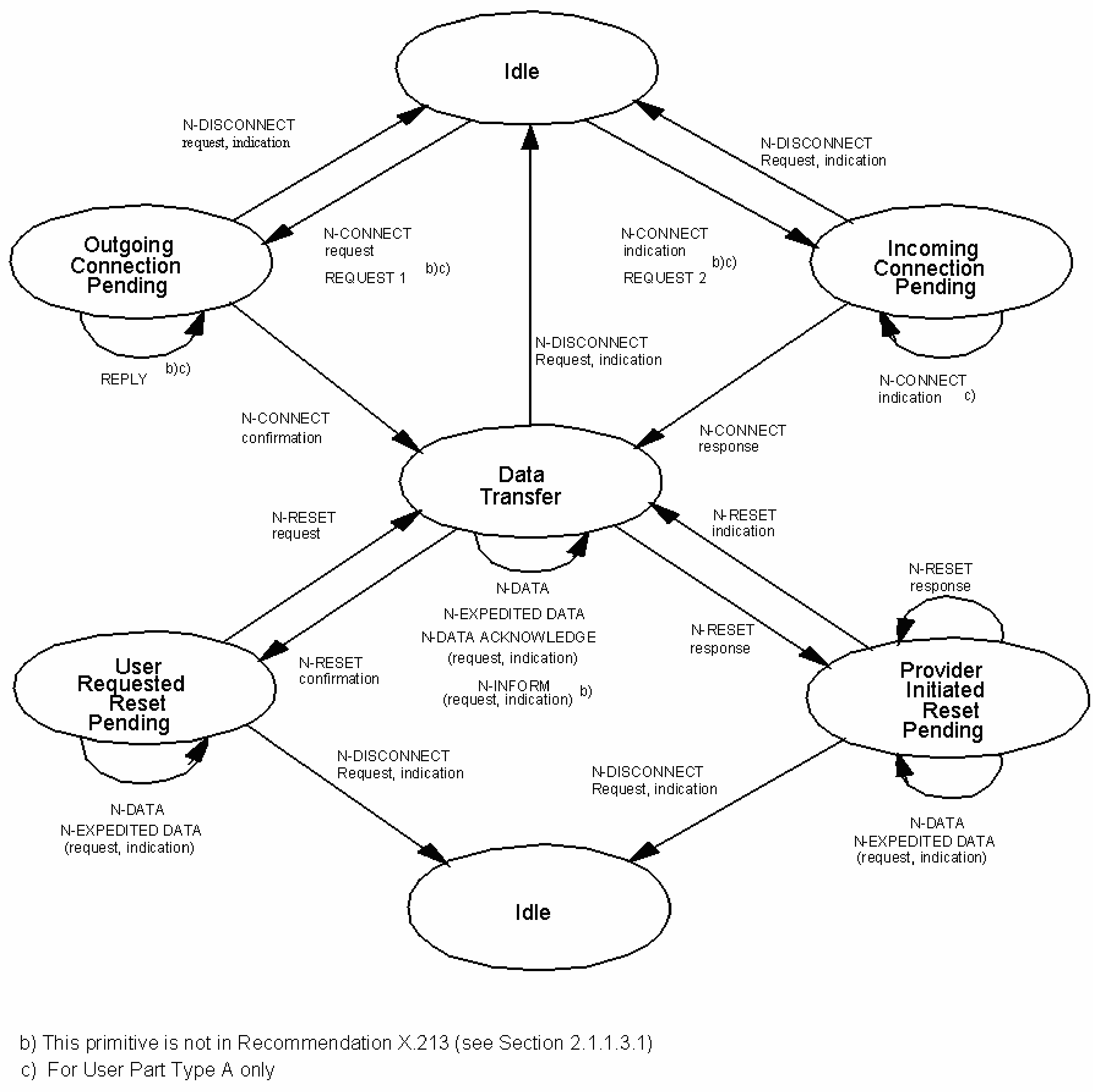


Figure 6/ATIS-1000112.1 - State Transition Diagram for the Sequence of Primitives at a Connection Endpoint (Basic Transitions)

Annex A

(informative)

ANNEX A NETWORK LAYER SERVICES

A.1 Glossary

(See T1.110.2.)

A.2 Relationship Among the Terms "Layer," "Entity," "Layer Service," "Layer Boundary," "Layer Service Primitive," and "Peer Protocol"

The basic purpose of a given layer is to offer a service (i.e., the layer service) to the layer above (see Figure A.1/ATIS-1000112.1). The "(N)" layer service is composed of "(N)" layer service elements and the cumulative results of the services of the underlying layers. These layer service elements are invoked or indicated by means of layer service primitives. There are four types of layer service primitives that constitute the interactions across the layer boundary. These are:

1. *Request*. A primitive issued by a service user to invoke a service element
2. *Indication*. A primitive issued by a service provider to advise that a service element has been invoked by the service user at the peer service access point or by the service provider
3. *Response*. A primitive issued by a service user to complete at a particular service access point some service element whose invocation has been previously indicated at that service access point
4. *Confirm*. A primitive issued by a service provider to complete at a particular service access point some service element previously invoked by a request at that service access point

There may be more than one entity in the same layer in the same system. Peer protocols, however, are only employed to exchange information between entities in the same layer but in different systems. (Additional explanation for information exchange between two entities in the same layer and in one and the same system is for further study.)

A.3 Data Transport

An SCCP message between two peers consists of the:

1. Network Protocol Control Information (NPCI); and
2. Network Service Data Unit (NSDU).

The NPCI supports the joint operating of the SCCP-peer entities within the two nodes communicating with each other.

The NSDU contains a certain amount of information from the NSP-User that has to be transferred between two nodes using the service of the SCCP. The NPCI and the NSDU are put together and transferred as a message (Figure A.2/ATIS-1000112.1). If there is too much user data to be transferred within one message, user data is segmented into a number of portions. Each portion is mapped to a separate message, consisting of an NPCI and an NSDU (see Figure A.3/ATIS-1000112.1).

A.4 Flow Control

The rate of data flow may be controlled:

1. Between adjacent layers (i.e., between the NSP-user and the SCCP); or
2. Between the two peers.

The flow control function permits a receiving entity to limit the data flow from the sending entity.

A.5 Sequencing

The user of the SCCP may ask for preservation of a given sequence of NSDUs.

The MTP provides sequence integrity for messages using the same SLS code (see ATIS-1000111.4). The SCCP also provides a means for maintaining sequence integrity.

A.6 Acknowledgment

To achieve a higher probability of detecting a message loss than is already provided by the MTP, an acknowledgment function may be used. The receiver of a message has to inform the sender of its correct receipt. The message needs to be uniquely identifiable. This may be achieved by a numbering mechanism.

A.7 Reset

To recover from a loss of synchronization between two entities, a reset function has to be provided to return to a predefined state with possible loss or duplication of data.

A.8 Restart

Definition for further study.

A.9 Expedited Data

Expedited Data are transferred with priority and bypass the normal data flow. The expedited data flow is necessarily very small, so that simpler flow control may be applied.

A.10 Routing

This function is based on the called party address information (and any optional routing parameters). Depending on the type of address, the routing function has to:

1. Evaluate the address information.
2. Translate it to an address type that can be used within the common channel network.
3. Check the availability of the addressee.
4. Check the need for an association of connection sections.

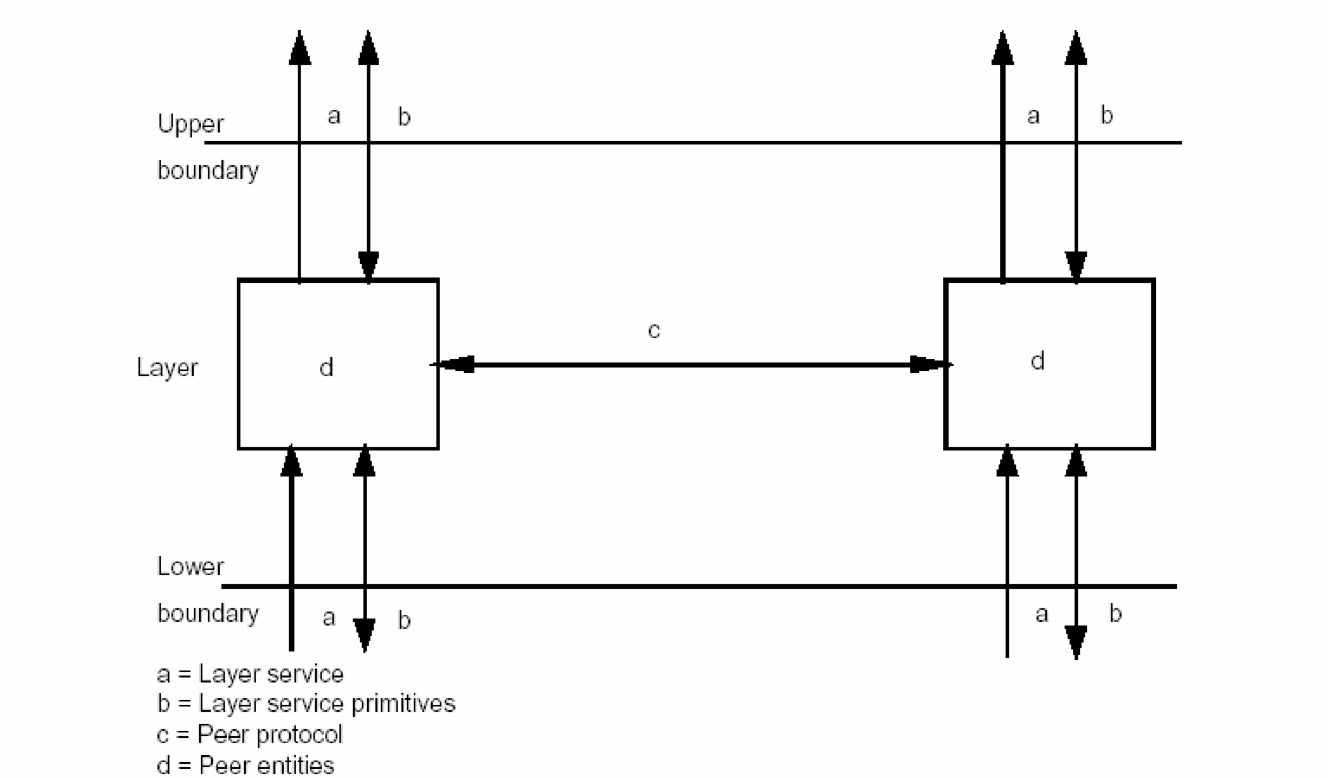


Figure A- 1/ATIS-1000112.1 - Layer and Peer Relationships

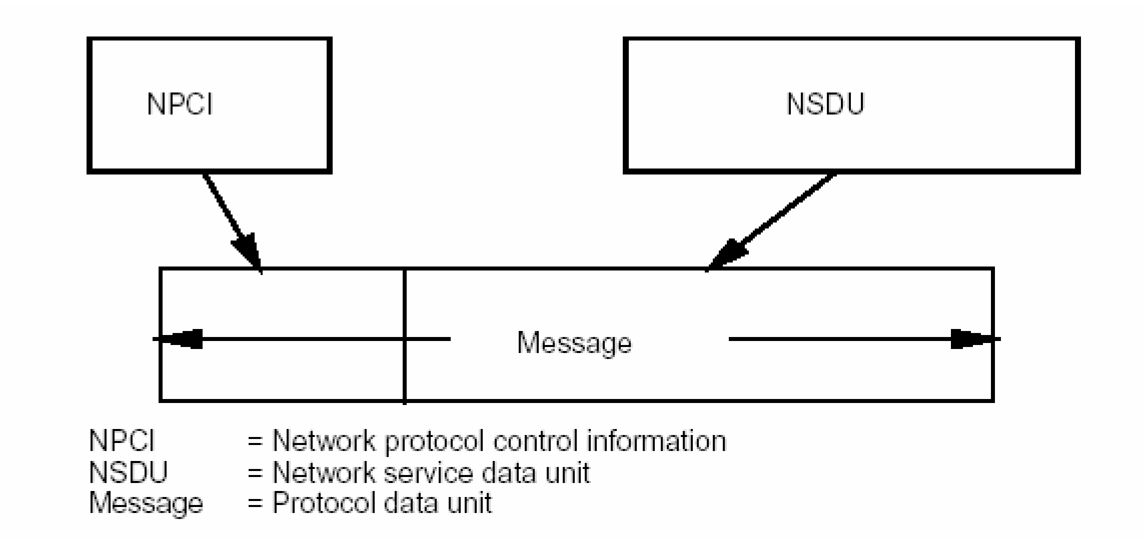


Figure A- 2/ATIS-1000112.1 - Relation between NSDU and Message with Neither Segmenting Nor Blocking

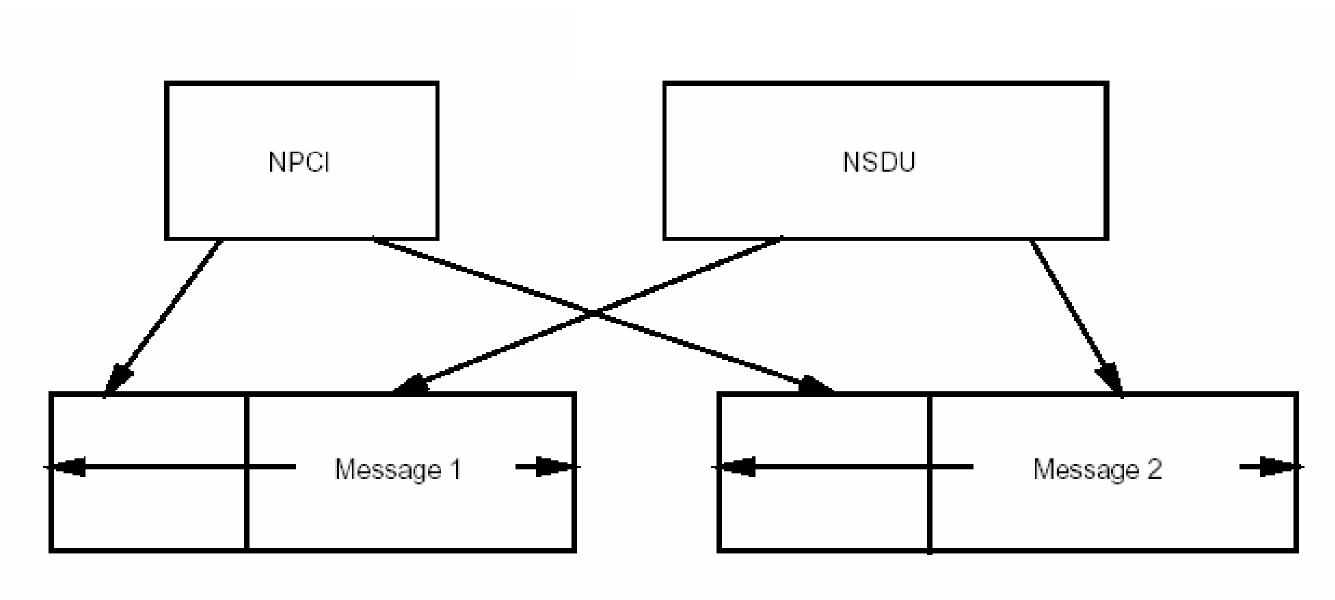


Figure A- 3/ATIS-1000112.1 - Segmenting

Chapter 2
Definitions and Functions of
Signaling Connection Control Part Messages

Table of Contents

Table of Tables

American National Standard for Telecommunications –

Definitions and Functions of Signaling Connection Control Part Messages

1 SCOPE, PURPOSE, AND APPLICATION[1]

This chapter provides the definitions and functions of Signaling Connection Control Part (SCCP) messages and information elements. The SCCP messages are used by the peer-to-peer SCCP protocol. The meaning and definition of the various information elements contained in these messages are specified in clause 3. The actual inclusion of these information elements in a given message depends on the class of protocol and is specified in clause 4.

This chapter may contain requirements that reference other American National Standards. If so, when the American National Standards referenced in the requirements are superseded by revisions approved by the ANSI, the revisions shall apply.

2 SIGNALING CONNECTION CONTROL PART MESSAGES

2.1 Connection Confirm (CC)

A Connection Confirm (CC) message is sent by the called SCCP to indicate to the calling SCCP that it has performed the setup of the signaling connection. On reception of a Connection Confirm message, the calling SCCP completes the setup of the signaling connection, if possible.

This message is used during the connection establishment phase for protocol class 2 or 3.

2.2 Connection Request (CR)

A Connection Request (CR) message is sent by the calling SCCP to the called SCCP to request the setting up of a signaling connection between the two entities. The required characteristics of the signaling connection are carried in various parameter fields. On reception of a Connection Request message, the called SCCP initiates the setup of the signaling connection, if possible.

This message is used during the connection establishment phase for protocol class 2 or 3.

[1] A "|" in the right margin indicates a change from ATIS-1000112.2-2001.

2.3 Connection Refused (CREF)

A Connection Refused (CREF) message is sent by the called SCCP or an intermediate node SCCP to indicate that the setup of the signaling connection has been refused.

This message is used during the connection establishment phase for protocol class 2 or 3.

2.4 Data Acknowledgment (AK)

A Data Acknowledgment (AK) message is used to control the window flow control mechanism which has been selected for the data transfer phase.

This message is used during the data transfer phase of protocol class 3.

2.5 Data Form 1 (DT1)

The Data Form 1 (DT1) message is sent by either end of a signaling connection to pass transparently SCCP user data between two SCCP nodes.

This message is used during the data transfer phase of protocol class 2 only.

2.6 Data Form 2 (DT2)

The Data Form 2 (DT2) message is sent by either end of a signaling connection to pass transparently SCCP user data between two SCCP nodes and to acknowledge messages flowing in the other direction.

This message is used during the data transfer phase of protocol class 3 only.

2.7 Expedited Data (ED)

An Expedited Data (ED) message functions as a Data Form 2 message but includes the ability to bypass the flow control mechanism that has been selected for the data transfer phase. It may be sent by either end of the signaling connection.

This message is used during the data transfer phase of protocol class 3 only.

2.8 Expedited Data Acknowledgment (EA)

An Expedited Data Acknowledgment (EA) message is used to acknowledge and Expedited Data message. Every ED message has to be acknowledged by an EA message before another ED message may be sent.

This message is used during the data transfer phase of protocol class 3 only.

2.9 Inactivity Test (IT)

An Inactivity Test (IT) message may be sent periodically by either end of a signaling connection to check if this signaling connection is active at both ends, and to audit the consistency of connection data at both ends.

This message is used in protocol classes 2 and 3.

2.10 Protocol Data Unit Error (ERR)

A Protocol Data Unit Error (ERR) message is sent on detection of any protocol errors.

This message is used in protocol classes 2 and 3.

2.11 Released (RLSD)

The Released (RLSD) message is sent in the forward or backward direction, to indicate that the sending SCCP wants to release the signaling connection and the associated resources at the sending SCCP have been brought into the disconnect pending condition. It also indicates that the receiving node should release the connection and any other resources associated with it.

This message is used during the connection release phase of protocol classes 2 and 3.

2.12 Release Complete (RLC)

The Release Complete (RLC) message is sent in response to the Released (RLSD) message, indicating that the Released message has been received, and that the appropriate procedures have been completed.

This message is used during the connection release phase of protocol classes 2 and 3.

2.13 Reset Confirmation (RSC)

A Reset Confirmation (RSC) message is sent in response to a Reset Request (RSR) message to indicate that the RSR message has been received and the appropriate procedures have been completed.

This message is used during the data transfer phase of protocol class 3.

2.14 Reset Request (RSR)

A Reset Request (RSR) message is sent to indicate that the sending node wants to initiate a reset procedure (re-initialization of sequence numbers) with the receiving SCCP.

This message is used during the data transfer phase of protocol class 3.

2.15 Unitdata (UDT)

A SCCP wanting to send data in a connectionless mode uses a Unitdata (UDT) message.

It is used for protocol classes 0 and 1.

2.15A Extended Unitdata (XUDT)

A SCCP wanting to send data in a connectionless mode, but including optional parameters uses the Extended Unitdata (XUDT) message. As a default, its treatment is identical to that of a UDT message.

It is used for protocol classes 0 and 1.

2.15B Long UnitData (LUDT)

A Long Unitdata (LUDT) message is used by the SCCP to send data (along with optional parameters) in a connectionless mode. Depending on the capability of the underlying MTP-3 and link level protocols, it allows sending of NSDU sizes up to 3904 octets without segmentation.

It is used for protocol classes 0 and 1.

2.16 Unitdata Service (UDTS)

Whenever it is not possible to route a UDT message and the message return on error option is included, a Unitdata Service (UDTS) message is sent back to the originator. Exceptionally and subjected to protocol interworking considerations, a UDTS might equally be used in response to an XUDT or LUDT message.

It is used for protocol classes 0 and 1.

2.16A Extended Unitdata Service (XUDTS)

Whenever it is not possible to route an XUDT message and the message return on error option is included, an Extended Unitdata Service (XUDTS) message is sent back to the originator. Exceptionally and subjected to protocol interworking considerations, an XUDTS might equally be used in response to an UDT or LUDT message.

It is used for protocol classes 0 and 1.

2.16B Long UnitData Service (LUDTS)

A Long Unitdata Service (LUDTS) message is used to indicate to the originating SCCP that a LUDT cannot be delivered to its destination. A LUDTS message is sent only when the return message on error option in the LUDT is set.

It is used for protocol classes 0 and 1.

3 MESSAGES FOR SCCP SUBSYSTEM MANAGEMENT

3.1 Subsystem-Allowed (SSA)

The Subsystem-Allowed (SSA) message is sent to concerned destinations to inform SCCP Management (SCMG) at the destinations that a subsystem which was formerly prohibited is now allowed. Upon receipt of a SSA message, the SCCP subsystem status is updated.

3.2 Subsystem-Prohibited (SSP)

The Subsystem-Prohibited (SSP) message is sent to concerned destinations to inform SCMG at the destinations of the failure of a subsystem. Upon receipt of a SSP message, the SCCP subsystem status is updated.

3.3 Subsystem-Status-Test (SST)

The Subsystem-Status-Test (SST) message is sent to verify the status of a subsystem marked prohibited.

3.4 Subsystem-Out-of-Service-Request (SOR)

When a subsystem wishes to go out-of-service, the request is transferred by means of a Subsystem-Out-of-Service-Request (SOR) message between the SCMG function at that node and the SCMG at the replicated subsystem's node(s). The purpose of the SOR message is to allow subsystems to go out-of-service without degrading performance of the network.

3.5 Subsystem-Out-of-Service-Grant (SOG)

When SCMG receives a SOR message, if both it and the backup of the affected subsystem agree to the request, a Subsystem-Out-of-Service-Grant (SOG) message is sent to the SCMG function associated with the affected subsystem.

3.6 Subsystem-Backup-Routing (SBR) (Optional)

If a subsystem becomes prohibited at an end node adjacent to an intermediate node, a Subsystem-Backup-Routing (SBR) message is sent by SCMG at the intermediate node to the SCMG associated with the backup subsystem. The SBR message is sent prior to rerouting traffic to the backup subsystem. The purpose of the SBR message is to provide additional network connectivity information so that SCMG at the end node may determine the traffic mix received for a subsystem.

3.7 Subsystem-Normal-Routing (SNR) (Optional)

If a subsystem that was prohibited becomes allowed at an end node adjacent to an intermediate node, a Subsystem-Normal-Routing (SNR) message is sent by the SCMG at the intermediate node to the SCMG associated with the backup subsystem. The SNR message is sent, prior to rerouting traffic to the primary subsystem, to the backup of the now allowed subsystem. This allows the SCMG at the end node to update the traffic mix information that the subsystem is receiving.

3.8 Subsystem-Routing-Status-Test (SRT) (Optional)

The Subsystem-Routing-Status-Test (SRT) message is sent to verify the routing status of a subsystem marked backup routed.

4 SCCP PARAMETERS

4.1 Calling/called party address

The "calling/called party address" parameter field contains enough information to uniquely identify the origination/destination signaling point and/or the SCCP service access point.

It can be any combination of a global title (e.g., dialed digits), a Signaling Point Code (SPC), and a subsystem number. In order to allow the interpretation of this address, it begins with an address indicator that indicates which information elements are present.

The address indicator also includes a routing indicator specifying if translation is required, a global title indicator specifying global title format, and a national/international indicator specifying use of national or international coding methods.

The "calling/called party address" parameter field has two different meanings depending on whether it is included in a connection-oriented or connectionless message.

For a connection-oriented message these fields have a global significance (i.e., independent of the direction the message is going).

For a connectionless message, these fields have significance dependent on the direction the message is going (just as for OPC and DPC).

4.2 Credit

The "credit" parameter field is used in the acknowledgments to indicate to the sender how many messages it may send. It is also used in the CR and CC message to indicate the proposed and selected credit, and in the IT message to audit the consistency of this connection data at both ends of a connection section.

4.3 Data

The "data" parameter field contains information coming from upper layers or from SCCP management.

In connectionless and connection-oriented messages, the data parameter field contains information coming from upper layers.

Information coming from SCCP management will be contained in the data parameter field of a UDT message. In this case, the data parameter field of the UDT message will only contain the SCCP management message.

4.4 Diagnostic

For connectionless protocol classes, the "diagnostic" parameter field has been renamed as the "return cause" parameter field. For connection oriented protocol classes, the "diagnostic" parameter field is for further study.

4.5 End of optional parameters

The "end of optional parameters" parameter field is used in any message containing optional parameters to indicate where the part allocated to these optional parameters ends.

4.6 Error cause

The "error cause" parameter field is used in the Protocol Data Unit Error (ERR) message in order to indicate what is the exact protocol error.

4.7 Local reference number (source/destination)

The "local reference number (Source/Destination)" parameter field uniquely identifies a signaling connection in a node. It is an internal working number chosen by each node independently from the destination node. At least one local reference number is to be found in any message exchange on a signaling connection section.

4.8 Message type code

The "message type code" parameter field is to be found in all the messages. It uniquely identifies the type of the messages (CR, CC,... as described in clause 1).

4.9 Protocol class

For connection-oriented protocol classes the "protocol class" parameter field is used during the connection establishment phase: it is negotiated between the two end SCCPs. It is also used during the data transfer phase to audit the consistency of this connection data at both ends of a connection section.

For connectionless protocol classes the "protocol class" field is used also to indicate whether or not a message should be returned on error occurrence.

4.10 Receive sequence number

The "receive sequence number" parameter field P(R) is used in the data acknowledgment message to indicate the lower edge of the window.

It also indicates that at least all messages numbered up to and including P(R) - 1 are accepted.

4.11 Refusal cause

The "refusal cause" parameter field is used in a Connection Refused message to indicate the reason why the connection was refused.

4.12 Release cause

The "release cause" parameter field is used in the Released message to indicate the reason of the release.

4.13 Reset cause

The "reset cause" parameter field is used in the Reset Request message to indicate the reason why a reset procedure is invoked.

4.14 Return cause

For connectionless protocol classes, the “return cause" parameter field is used to indicate the reason why a message was returned.

4.15 Segmenting/reassembling

The "segmenting/reassembling" parameter field is used in the data message for the segmenting and reassembling function. It is the more data indicator (M-bit).

It is set to one in a data message to indicate that more user data will follow in a subsequent message.

It is set to zero in a data message to indicate that the data in this message forms the end of a complete data sequence.

4.16 Sequencing/segmenting

The "sequencing/segmenting" parameter field contains the information necessary for the following functions: sequence numbering, flow control, segmenting and reassembling.

It consists of: the sequence number of the message sent, P(S); the receive sequence number, P(R); and the more data indicator (M-bit).

4.17 SCCP hop counter

The "SCCP hop counter" parameter is used to count the number of SCCP relay points (hops) a message passes through, and can be used to detect the possible looping of messages.

4.18 Segmentation

The "segmentation" parameter field is used to indicate that a SCCP message has been segmented, or -- in case of the LUDT(S) -- that it may undergo segmenting at an interworking node where the services offered by MTP-3 are different as a result of the capability of the link level protocols. The parameter also contains all the information necessary to allow the correct reassembly of the message.

4.19 Intermediate Signaling Network Identification (ISNI)

The ISNI parameter field is used to indicate the need of an ISNI routing function at an ISNI-capable SCCP relay node, and to identify the actual networks traversed by the signaling messages. The parameter contains a list of two-octet Network Identifiers (NIDs); an indicator of the type ISNI routing: constrained, suggested, or neither; an indicator requesting a logged record of the actual networks traversed by the signaling messages; a counter dynamically incremented to indicate which NID should be used for routing and identification; and a type indicator to indicate a Type 0 or 1 ISNI parameter.

4.20 Long Data

The ‘Long Data’ parameter is a ‘data’ parameter with a two octet length indicator. It allows sending of up to 3904 octets in a single LUDT or LUDTS message, depending on the capability of the underlying MTP Level 3 and link level protocols.

4.21 Intermediate Network Selection (INS)

The INS parameter field is used to indicate the need of an INS routing function at an INS-capable SCCP relay node. The parameter contains an indicator of the type of routing information: SS7 or network specific; NIDs: specifying the routing information; an indicator of the type of INS routing to be used: constrained, suggested, or neither constrained nor suggested; and a counter that provides an imaginary “pointer” to locate the routing information.

4.22 Message Type Interworking (MTI)

The Message Type Interworking (MTI) parameter contains an Original Message Type field specifying the message type before a message change and a drop option field that indicates whether the Message Type Interworking parameter could be dropped.

The Message Type Interworking parameter is an optional parameter of SCCP connectionless services.

5 Parameters for SCCP Subsystem Management

5.1 Affected subsystem number

The "affected subsystem number" identifies a subsystem which is failed, withdrawn, congested, or allowed. In the case of the SST and SRT messages, it also identifies the subsystem being audited. In the case of SOR or SOG messages, it identifies a subsystem requesting to go out of service.

5.2 Affected point code

The "affected point code" identifies a point code where the affected subsystem is located.

5.3 Subsystem multiplicity indicator

The "subsystem multiplicity indicator" is used in SCCP management messages to indicate the number of associated replicated subsystems.

6 INCLUSION OF FIELDS IN THE MESSAGES

The inclusion of the information elements specified in clause 2 in the various messages specified in clause 1 according to their type depends on the class of protocol. SCCP messages are specified in Table 1 and SCCP management messages are specified in Table 2. SCCP management messages are embedded in the "user data" parameter of the UDT message.

The following applies to Table 1/ATIS-1000112.2 and Table 2/ATIS-1000112.2:

m = mandatory field (previously labeled MAN);

o = optional field (previously labeled OPT), which is included in a message when needed.

Table 1/ATIS-1000112.2 - Inclusion of Fields in Messages (Sheet 1 of 3)

Messages/ Parameter Fields	**CR**	**CC**	**CREF**	**RLSD**	**RLC**	**DT1**	**DT2**	**AK**	**ED**
Message Type Code	m	m	m	m	m	m	m	m	m
Destination local ref.		m	m	m	m	m	m	m	m
Source local ref.	m	m		m	m				
Called party address	m	o	o						
Calling party address	o								
Protocol class	m	m							
Segmenting/ Reassembling						m			
Receive sequence no.								m	
Sequencing/ Segmenting							m		
Credit	o	o						m	
Release Cause				m					
Return Cause									
Reset cause									
Error cause									
Data	o	o	o	o		m	m		m
Refusal cause			m						
End of opt. parameters	o	o	o	o					
SCCP Hop Counter	o								
Segmentation									
ISNI									
Long Data									
INS									
MTI									

Table 1/ATIS-1000112.2 - Inclusion of Fields in Messages (Sheet 2 of 3)

Messages/ Parameter Fields	EA	RSR	RSC	ERR	IT	UDT	XUDT	UDTS	XUDTS
Message Type Code	m	m	m	m	m	m	m	m	m
Destination local ref.	m	m	m	m	m				
Source local ref.		m	m		m				
Called party address						m	m	m	m
Calling party address						m	m	m	m
Protocol class					m	m	m		
Segmenting/ Reassembling									
Receive sequence no.									
Sequencing/ Segmenting					M[1]				
Credit					M[1]				
Release Cause									
Return Cause								m	m
Reset cause		m							
Error cause				m					
Data						m	m	m	m
Refusal cause									
End of opt. parameters							o		o
SCCP Hop Counter							m		m
Segmentation							o		o
ISNI							o		o
Long Data									
INS							o		o
MTI							o		o

[1] Information in these fields is ignored if the protocol class parameter indicates class 2.

Table 1/ATIS-1000112.2 - Inclusion of Fields in Messages (Sheet 3 of 3)

Messages/ Parameter Fields	**LUDT**	**LUDTS**
Message Type Code	m	m
Destination local ref.		
Source local ref.		
Called party address	m	m
Calling party address	m	m
Protocol class	m	
Segmenting/Reassembling		
Receive sequence no.		
Sequencing/Segmenting		
Credit		
Release Cause		
Return Cause		m
Reset cause		
Error cause		
Data		
Refusal cause		
End of opt. parameters	o	o
SCCP Hop Counter	m	m
Segmentation	o[2)]	o
ISNI	o	o
Long Data	m	m
INS	o	o
MTI		

[2)] The segmentation parameter must be included by the originating node, if interworking is expected with an MTP network or part of an MTP network with different capabilities (i.e., different link level protocols).

Table 2/ATIS-1000112.2 - SCCP Management Messages

Messages Fields	**SSP**	**SSA**	**SST**	**SOR**	**SOG**	**SBR**	**SNR**	**SRT**
SCMG format ID	m	m	m	m	m	m	m	m
Affected SSN	m	m	m	m	m	m	m	m
Affected PC	m	m	m	m	m	m	m	m
Subsystem multiplicity indicator	m	m	m	m	m	m	m	m

Chapter 3
Signaling Connection Control Part Formats and Codes

Table of Contents

Table of Figures

Table of Tables

American National Standard for Telecommunications –

Signaling Connection Control Part Formats and Codes

1 Scope, Purpose, and Applications[1]

This chapter describes the formats and codes used for Signaling Connection Control Part (SCCP) messages and fields. The SCCP messages are carried on the signaling data link by means of Signal Units the format of which is described in ATIS-1000111.3, clause 2.2.

The Service Information Octet (SIO) format and coding is described in ATIS-1000111.4, clause 13.2. The Service Indicator is coded 0011 for the SCCP. There are three annexes in this chapter. Annex A is normative and is considered part of the SCCP standard. Annexes B and C are informative and are not considered part of the SCCP standard.

The Signaling Information Field (SIF) of each Message Signal Unit containing an SCCP message consists of an integral number of octets.

A message consists of the following parts (see Figure 1/ATIS-1000112.3):

1. The routing label;
2. The message type;
3. The mandatory fixed part;
4. The mandatory variable part; and
5. The optional part, which may contain fixed length and variable length fields.

The description of the various parts is contained in the following clauses. SCCP Management messages and codes are provided in clause 5 of this chapter.

This chapter may contain requirements that reference other American National Standards. If so, when the American National Standards referenced in the requirements are superseded by revisions approved by ANSI, the revisions shall apply.

1.1 Routing label

The standard routing label specified in ATIS-1000111.4, clause 2.2 is used. The rules for the generation of the signaling link selection (SLS) code are described in ATIS-1000112.1, clause 2.2.1.

[1] A "|" in the right margin indicates a change from ATIS-1000112.3-2001.

1.2 Message type code

The message type code consists of a one octet field, and is mandatory for all messages. The message type code uniquely defines the function and format of each SCCP message. The allocation of message type codes, with reference to the appropriate descriptive clause of this Recommendation is summarized in Table 1/ATIS-1000112.3. Table 1/ATIS-1000112.3 also contains an indication of the applicability of the various message types to the relevant classes of protocol.

1.3 Formatting principles

Each message consists of a number of parameters listed and described in clause 3. Each parameter has a "name" which is coded as a single octet (see clause 3). The length of a parameter may be fixed or variable, and a "length indicator" of one octet for each parameter may be included as described below.

The length indicator of the Long Data parameter shall be two octets, with the less significant octet preceding the transmission of the more significant octet.

The detailed format is uniquely defined for each message type as described in clause 4.

A general format diagram is shown in Figure 2/ATIS-1000112.3.

1.4 Mandatory fixed part

Those parameters that are mandatory and of fixed length for a particular message type will be contained in the mandatory fixed part. The position, length, and order of the parameters is uniquely defined by the message type. Thus, the names of the parameters and the length indicators are not included in the message.

1.5 Mandatory variable part

Mandatory parameters of variable length will be included in the mandatory variable part. The name of each parameter and the order in which the pointers are sent is implicit in the message type. Parameter names are, therefore, not included in the message. Pointers are used to indicate the beginning of each parameter. Because their position is indicated by the pointer values, the parameters themselves may be sent in an order different from that of the pointers. Each pointer is encoded as a single octet, or two octets in the case of LUDT or LUDTS. In the case of the two-octet pointer, the less significant octet shall be transmitted before the more significant octet. The details of how pointers are encoded are found in clause 2.3. The number of parameters, and thus the number of pointers, is uniquely defined by the message type.

A pointer is also included to indicate the beginning of the optional part. If the message type indicates that no optional part is allowed, then this pointer will not be present. If the message type indicates that an optional part is possible, but there is no optional part included in this particular message, then a pointer field containing all zeros will be used.

All the pointers are sent consecutively at the beginning of the mandatory variable part. Each parameter contains the parameter length indicator followed by the contents of the parameter.

All the pointers indicating the beginning of the mandatory variable parameters and the pointer to the beginning of the optional part shall ensure that the parameters are contiguous and "gaps" shall not be left in between parameters in generating messages. The treatment of gaps within received messages is specified in ATIS-1000112.4.

1.6 Optional part

The optional part consists of parameters that may or may not occur in any particular message type. Both fixed length and variable length parameters may be included. Optional parameters may be transmitted in any order.[2] Each optional parameter will include the parameter name (one octet) and the length indicator (one octet) followed by the parameter contents.

1.7 End of optional parameters octet

After all optional parameters have been sent, an "end of optional parameters" octet containing all zeros will be transmitted. This octet is only included if optional parameters are present in the message.

1.8 Order of transmission

Since all the parameters consist of an integral number of octets, the formats are presented as a stack of octets. The first octet transmitted is the one shown at the top of the stack and the last is the one at the bottom (see Figure 2/ATIS-1000112.3).

Within each octet, the bits are transmitted with the least significant bit first. For multiple octet fields (e.g., a signaling point code within an address parameter), the least significant octet is sent first.

1.9 Coding of spare bits

Spare bits are coded 0 unless indicated otherwise at the originating node. At intermediate nodes, they are passed transparently. At the destination node, they need not be examined.

1.10 National message types and parameters

If message type codes and parameter codes are required for national uses, the codes chosen should be from the highest code downwards (i.e., starting at code 11111110). Code 11111111 is reserved for future use.

2 CODING OF THE GENERAL PARTS

2.1 Coding of the message type

The coding of the message type is shown in Table 1/ATIS-1000112.3.

---

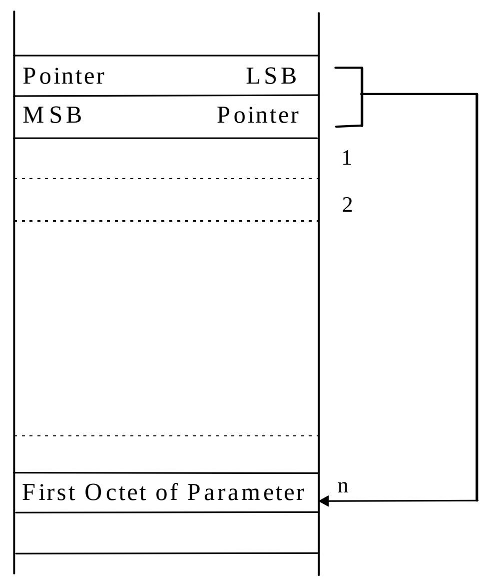
[2] It is for further study if any constraint in the order of transmission will be introduced.

2.2 Coding of the length indicator

The length indicator field is binary coded to indicate the number of octets in the parameter content field. The length indicator does not include the parameter name octet or the length indicator octet.

2.3 Coding of the pointers

The pointer value (in binary) gives the number of octets between the most significant octet of the pointer itself (*not* included) and the first octet (included) of the parameter associated with that pointer[3] as shown in the following diagram.



The pointer value all zeros is used to indicate that, in the case of optional parameters, no optional parameter is present.

3 SCCP PARAMETERS

The parameter name codes are given in Table 2/ATIS-1000112.3 with reference to the subclauses in which they are described.

[3] For example, a pointer value of "00000001" indicates that the associated parameter begins in the octet immediately following the most significant octet of the pointer. A pointer value of "00001010" indicates that ten octets of information exist between the most significant octet of the pointer octet (not included) and the first octet of the parameter associated with that pointer (included). A two-octet pointer value of “00000000 00001010” indicates that ten octets of information exist between the most significant octet of the pointer (not included) and the first octet of the parameter associated with that pointer (included).

3.1 End of optional parameters

The "end of optional parameters" parameter field consists of a single octet containing all zeros.

3.2 Destination local reference

The destination local reference parameter field is a three-octet field containing a reference number that is included in a message to allow the node receiving the message to identify the message with a particular connection section.

The coding "all ones" is reserved, its use is for further study.

3.3 Source local reference

The source local reference parameter field is a three-octet field containing a reference number which is included in a message to allow the node receiving the message to determine a destination local reference for messages it sends in the reverse direction. It may also be used for verification of connection status.

The coding "all ones" is reserved, its use is for further study.

3.4 Called party address

The called party address is a variable length parameter. Its structure is shown in Figure 3/ATIS-1000112.3.

3.4.1 Address indicator

The address indicator indicates the type of address information contained in the address field (see Figure 4/ATIS-1000112.3). The address consists of one or any combination of the following elements:

1. Signaling point code;
2. Global title (for instance, dialed digits); or
3. Subsystem number.

A "1" in bit 1 indicates that the address contains a subsystem number.

A "1" in bit 2 indicates that the address contains a signaling point code.

Bits 3-6 of the address indicator octet contain the global title indicator, which is encoded as follows:

Bits	6543	
	0000	No global title included
	0001	Global title includes translation type, numbering plan and encoding scheme
	0010	Global title includes translation type
	0011 to 0100	not assigned for U.S. networks
	0101 to 0111	spare international
	1000 to 1110	spare national
	1111	reserved for extension

When a global title is used in the called party address, the called party address should also contain a subsystem number. This serves to simplify message re-formatting following global title translation. The subsystem number should be encoded "00000000" when the subsystem number is not known, e.g., before translation.

Bit 7 of the address indicator octet contains routing information identifying which address element should be used for routing[4].

A "0" in bit 7 indicates that an SCCP translation is required and therefore that routing should be based on the global title in the address (and any optional routing parameters).

A "1" in bit 7 indicates that routing should be based on the destination point code in the routing label and the subsystem number information in the called party address.

Bit 8 of the address indicator octet is designated for national use and will be used as follows:

A "0" in Bit 8 will indicate that the address is international and that both the address indicator and the address are coded according to international specifications.

A "1" in Bit 8 will indicate that the address is national and that both the address indicator and the address are coded according to national specifications.

[The ordering of the subsystem number indicator field and the point code indicator field are in a reverse order in the ITU-T format.]

3.4.2 Address

The various elements, when provided, occur in the order: subsystem number, signaling point code, global title, as shown in Figure 4A/ATIS-1000112.3.[5]

---

[4] Detailed procedures for message routing are given in ATIS-1000112.4, clauses 2.2.1.1 and 2.2.1.2.

[5] The ordering of the subsystem number and the point code are in a reverse order in the ITU-T format.

3.4.2.1 Subsystem number

The subsystem number (SSN) identifies a SCCP user function and, when provided, consists of one octet coded as follows:

Bits	87654321	
	00000000	SSN not known/not used
	00000001	SCCP Management
	00000010	reserved
	00000011	ISDN User Part
	00000100	OMAP
	00000101	Mobile Application Part (MAP)[6]
	00000110	Home Location Register (HLR)[6]
	00000111	Visited Location Register (VLR)[6]
	00001000	Mobile Switching Center (MSC)[6]
	00001001	Equipment Identification Register (EIR)[6]
	00001010	Authentication Center (AC)[6]
	00001011	Reserved (used in ITU-T for ISDN supplementary services)
	00001100	Reserved for international use
	00001101	Reserved (used in ITU-T for broadband ISDN edge-to-edge applications)
	00001110	Reserved (used in ITU-T for TC test responder)
	00001111 to 00011111	Reserved for international use
	00100000 to 11111110	Spare
	11111111	reserved for expansion

Network specific subsystem numbers should be assigned in descending order starting with "11111110."

3.4.2.2 Signaling point code

The Signaling Point Code (SPC), when provided as an address element (e.g., part of the Called Party Address) or as global title address information, is represented by three octets (see Figure 5/ATIS-1000112.3). The SPC is transmitted in the following order: Network Cluster Member, Network Cluster, and Network Identifier.

3.4.2.3 Global Title

The format of the global title is of variable length. Figure 6/ATIS-1000112.3 and Figure 6A/ATIS-1000112.3 show two possible formats for global title.

---

[6] These codes are assigned to the MAP application defined by EIA/TIA for North American networks.

3.4.2.3.1 Global Title Indicator = 0001[7]

The translation type is a one-octet field that is used to direct the message to the appropriate global title translation function.[8]

Translation type coding for indicator value 0001 is for further study.

The numbering plan for indicator value 0001 is encoded as follows:

Bits	8765	
	0000	unknown
	0001	ISDN/Telephony Numbering Plan (ITU-T Rec. E.164)
	0010	reserved
	0011	Data Numbering Plan (ITU-T Rec. X.121)
	0100	Telex Numbering Plan (ITU-T Rec. F.69)
	0101	Maritime Mobile Numbering Plan (ITU-T Rec. E.210,211)
	0110	Land Mobile Numbering Plan (ITU-T Rec. E.212)
	0111	ISDN/Mobile Numbering Plan (ITU-T Rec. E.214)
	1000 to 1001	spare
	1110	Private Network or Network Specific Numbering Plan[9]
	1111	reserved

The encoding scheme is encoded as follows:

Bits	4321	
	0000	unknown
	0001	BCD, Odd number of digits
	0010	BCD, Even number of digits
	0011 to 1111	spare

If the encoding scheme is binary coded decimal, the global title address information is encoded as shown in Figure 6B/ATIS-1000112.3.

---

[7] ITU-T uses global title indicator 0011 for the same format.

[8] A translation type may for instance imply a specific service to be provided by the SCCP-user, such as 800 number translation, or identify the category of service to be provided, for example, dialed number screening, password validation, or translation of digits to telephone network address.

[9] The use of this code point is restricted to be used by the serving network. Internetwork use of this code point should be mutually agreed on by the interconnecting network.

Each address signal is coded as follows:

0000	digit	0
0001	digit	1
0010	digit	2
0011	digit	3
0100	digit	4
0101	digit	5
0110	digit	6
0111	digit	7
1000	digit	8
1001	digit	9
1010	spare	
1011	code	11[10]
1100	code	12[10]
1101	spare	
1110	spare	
1111	ST(Reserved)[10]	

In case of an odd number of address signals a filler code 0000 is inserted after the last address signal.

3.4.2.3.2 Global Title Indicator = 0010

Figure 6A/ATIS-1000112.3 shows the format of the global title, if the global title indicator equals "0010."

The translation type is a one-octet field that is used to direct the message to the appropriate global title translation function.[8] The translation type may also imply the encoding scheme, used to encode the address information, and the numbering plan. Translation types are assigned as described in normative Annex A and informative Annex B.

3.5 Calling party address

The "calling party address" is a variable length parameter. Its structure is the same as the called party address.

For connection-oriented messages, when the calling party address is a mandatory parameter but is not available or must not be sent, the calling party address parameter only consists of the address indicator octet, where bits 1 to 7 are coded all zeroes.

The calling party address should be formatted by the originating node so that it will permit the destination and any intermediate node to use the calling party address as the called party address in a response message or in the return of the message if the network is unable to route the message to its destination.

If the called party address requires global title translation, causing the Originating Point Code in the routing label to change, then the calling party address should not contain SSN only.

---

[10] NOTE - The application of these codes in actual networks is for further study.

3.6 Protocol class

The "protocol class" parameter field is a four-bit field containing the protocol class.

Bits 1-4 are coded as follows:

bits	4321	
	0000	class 0
	0001	class 1
	0010	class 2
	0011	class 3

When Bits 1-4 are coded to indicate a connection-oriented protocol class (class 2, class 3), Bits 5-8 are spare.

When Bits 1-4 are coded to indicate a connectionless protocol class (class 0, class 1), Bits 5-8 are used to specify message handling as follows:

bits	8765	
	0000	discard message on error
	0001	
	to	spare
	0111	
	1000	return message on error
	1001	
	to	spare
	1111	

3.7 Segmenting/reassembling

The "segmenting/reassembling" parameter field is a one octet field and is structured as shown in Figure 7/ATIS-1000112.3.

Bits 8-2 are spare.

Bit 1 is used for the More Data indication and is coded as follows:

0 = no more data
1 = more data

3.8 Receive sequence number

The "receive sequence number" parameter field is a one octet field and is structured as shown in Figure 8/ATIS-1000112.3.

Bits 8-2 contain the Receive sequence number P(R) used to indicate the sequence number of the next expected message. P(R) is binary coded and bit 2 is the LSB.

Bit 1 is spare.

3.9 Sequencing/segmenting

The "sequencing/segmenting" parameter field consists of two octets and is structured as shown in Figure 9/ATIS-1000112.3.

Bits 8-2 of octet 1 are used for indicating the Send sequence number P(S). P(S) is binary coded and bit 2 is the LSB.

Bit 1 of octet 1 is spare.

Bits 8-2 of octet 2 are used for indicating the Receive sequence number P(R). P(R) is binary coded and bit 2 is the LSB.

Bit 1 of octet 2 is used for the More Data indication and is coded as follows:

0 = no more data
1 = more data

The "sequencing/segmenting" parameter field is used exclusively in protocol class 3.

3.10 Credit

The "credit" parameter field is a one-octet field used in the protocol classes that include flow control functions. It contains the window size value coded in pure binary.

3.11 Release cause

The "release cause" parameter field is a one-octet field containing the reason for the release of the connection.

The coding of the release cause field is as follows:

00000000	end user originated
00000001	end user busy
00000010	end user failure
00000011	SCCP user originated
00000100	remote procedure error
00000101	inconsistent connection data
00000110	access failure
00000111	access congestion
00001000	subsystem failure
00001001	subsystem congestion[11]
00001010	MTP failure
00001011	network congestion
00001100	expiration of reset timer
00001101	expiration of receive inactivity timer
00001110	reserved
00001111	unqualified
00010000	SCCP failure

[11] Procedures associated with subsystem congestion are for further study.

00010001	
to	spare
11111111	

3.12 Return cause (formerly Diagnostic)

In the "Unitdata Service," "Extended Unitdata Service," and “Long Unitdata Service” messages, the return cause field (formerly called the diagnostic parameter field) is a one octet field containing the reason for message return. Bits 1-8 are coded as follows:

bits	87654321	
	00000000	no translation for an address of such nature
	00000001	no translation for this specific address
	00000010	subsystem congestion[11]
	00000011	subsystem failure
	00000100	unequipped user
	00000101	MTP failure
	00000110	network congestion
	00000111	unqualified
	00001000	error in message transport (1)
	00001001	error in local processing (1)
	00001010	destination cannot perform reassembly (1)
	00001011	SCCP Failure
	00001100	SCCP hop counter violation ~~(1)~~
	00001101	segmentation not supported
	00001110	segmentation failure
	00001111	
	to	spare
	11110110	
	11110111	message change failure
	11111000	invalid INS routing request
	11111001	invalid ISNI routing request (1)
	11111010	unauthorized message
	11111011	message incompatibility
	11111100	cannot perform ISNI constrained routing (1)
	11111101	redundant ISNI constrained routing information (1)
	11111110	unable to perform ISNI identification (1)
	11111111	spare

(1) NOTE - Only applicable to XUDT and XUDTS messages

3.13 Reset cause

The "reset cause" parameter field is a one octet field containing the reason for the resetting of the connection.

The coding of the reset cause field is as follows:

bits	87654321	
	00000000	end user originated
	00000001	SCCP user originated
	00000010	message out of order - incorrect P(S)
	00000011	message out of order - incorrect P(R)
	00000100	remote procedure error - message out of window
	00000101	rem. proc. error - incorrect P(S) after (re)init.
	00000110	remote procedure error - general
	00000111	remote end user operational
	00001000	network operational
	00001001	access operational
	00001010	network congestion
	00001011	not obtainable
	00001100	unqualified
	00001101 to 11111111	spare

3.14 Error cause

The "error cause" parameter field is a one octet field containing the indication of the exact protocol error.

The coding of the error cause field is as follows:

bits	87654321	
	00000000	local ref. no. mismatch - unassigned destination LRN
	00000001	LRN mismatch - inconsistent source LRN
	00000010	point code mismatch
	00000011	service class mismatch
	00000100	unqualified
	00000101 to 11111111	spare

3.15 Refusal cause

The "refusal cause" parameter field is a one octet field containing the reason for the refusal of the connection.

bits	87654321	
	00000000	end user originated
	00000001	end user congestion
	00000010	end user failure
	00000011	SCCP user originated
	00000100	destination address unknown
	00000101	destination inaccessible
	00000110	network resource - QoS not available/non-transient

00000111	network resource - QoS not available/transient
00001000	access failure
00001001	access congestion
00001010	subsystem failure
00001011	subsystem congestion[11]
00001100	expiration of the connection establishment timer
00001101	incompatible user data
00001110	reserved
00001111	unqualified
00010000	SCCP hop counter violation
00010001	SCCP Failure
00010010	No translation for an address of such nature
00010011	Unequipped user
00010100 to 11111111	spare

3.16 Data

The "data" parameter field is a variable length field containing less than or equal to 252 octets SCCP-user data to be transferred transparently between the SCCP-user functions.

3.17 SCCP Hop Counter

The "SCCP hop counter" parameter is a one octet parameter that contains a counter that is decremented each time the message is processed by an SCCP relay point. Its structure is shown in Figure 11/ATIS-1000112.3. If decrementing the counter results in the value of zero, the SCCP initiates the appropriate error procedure. If "return on error" is indicated, an "SCCP hop counter violation" return code is provided. The initial value of the counter is set by the originator of the message. An initial value of less than 16 is recommended.

3.18 Segmentation

The "segmentation" parameter is a 4-octet parameter coded as shown in Figure 12 /ATIS-1000112.3.

Bit 8 of octet 1 is used for the "First segment" indication and is coded as follows:

0: in all segments but the first
1: in the first segment

Bit 7 of octet 1 is used to keep the in-sequence delivery option required by the SCCP user and is coded as follows:

0: not in-sequence delivery (class '0' selected)
1: in-sequence delivery (class '1' selected)

Bits 6 and 5 in octet 1 are spare bits.

Bits 4-1 of octet 1 are used to indicate the number of remaining segments. The values "0000" to "1111" are possible; the value "0000" indicates the last segment.

3.19 Intermediate Signaling Network Identification (ISNI)

The ISNI parameter is a variable length parameter. Its structure is shown in Figure 13/ATIS-1000112.3. The ISNI routing control octet is applicable to both Type 0 and 1 ISNI parameter formats; and the extension octet is applicable to Type 1 ISNI parameter format only. Figure 13A/ATIS-1000112.3 shows the fields in both octets.

3.20 Long Data

The “long data” parameter field is a variable length field containing SCCP-user data up to 3904 octets to be transferred transparently between the SCCP user functions. The “long data” parameter has a two-octet “length indicator” field.

3.21 Intermediate Network Selection (INS)

The INS parameter is a variable length parameter. Its structure is shown in Figure 14/ATIS-1000112.3.

3.22 Message Type Interworking

The “Message Type Interworking” is a 1-octet parameter coded as shown in Figure 15/ATIS-1000112.3.

4 SCCP MESSAGES AND CODES

4.1 General

In the following clauses, the format and coding of the SCCP messages is specified. For each message, a list of the relevant parameters is given in a tabular form.

For each parameter the table also includes:

- *A reference* to the clause where the formatting and coding of the parameter content is specified;
- *The type* of the parameter. The following types are used in the tables:
  - F = mandatory fixed length parameter
  - V = mandatory variable length parameter
  - O = optional parameter of fixed or variable length;
- *The length* of the parameter. The value in the table includes:
  - *For type F parameters*: the length, in octets, of the parameter content;
  - *For type V parameters*: the length, in octets, of the length indicator and of the parameter content. The minimum and the maximum lengths are indicated;
  - *For type O parameters*: the length, in octets, of the parameter name; length indicator; and parameter content.

For each message the number of pointers included is also specified.

For each message type, type F parameters and the pointers for the type V parameters must be sent in the order specified in the following tables.

4.2 Connection Request (CR)

The CR message contains:

1. The routing label;
2. Two pointers; and
3. The parameters indicated in Table 3/ATIS-1000112.3.

4.3 Connection Confirm (CC)

The CC message contains:

1. The routing label;
2. One pointer; and
3. The parameters indicated in Table 4/ATIS-1000112.3.

4.4 Connection Refused (CREF)

The CREF message contains:

1. The routing label;
2. One pointer; and
3. The parameters indicated in Table 5/ATIS-1000112.3.

4.5 Released (RLSD)

The RLSD message contains:

1. The routing label;
2. One pointer; and
3. The parameters indicated in Table 6/ATIS-1000112.3.

4.6 Release Complete (RLC)

The RLC message contains:

1. The routing label;
2. No pointers; and
3. The parameters indicated in Table 7/ATIS-1000112.3.

4.7 Data Form 1 (DT1)

The DT1 message contains:

1. The routing label;
2. One pointer; and
3. The parameters indicated in Table 8/ATIS-1000112.3.

4.8 Data Form 2 (DT2)

The DT2 message contains:

1. The routing label;
2. One pointer; and
3. The parameters indicated in Table 9/ATIS-1000112.3.

4.9 Data Acknowledgment (AK)

The AK message contains:

1. The routing label;
2. No pointers; and
3. The parameters indicated in Table 10/ATIS-1000112.3.

4.10 Unitdata (UDT)

The UDT message contains:

1. The routing label;
2. Three pointers; and
3. The parameters indicated in Table 11/ATIS-1000112.3.

4.10A Extended Unitdata (XUDT)

The XUDT message contains:

1. The routing label;
2. Four pointers, including a pointer to the optional part; and
3. The parameters indicated in Table 11/ATIS-1000112.3.

4.10B Long Unitdata (LUDT)

The LUDT message contains:

1. The routing label;
2. Four two-octets pointers; and
3. The parameters indicated in Table 11B/ATIS-1000112.3.

4.11 Unitdata Service (UDTS)

The UDTS message contains:

1. The label;
2. Three pointers; and
3. The parameters indicted in Table 12/ATIS-1000112.3.

4.11A Extended Unitdata Service (XUDTS)

The XUDTS message contains:

1. The label;
2. Four pointers, including a pointer to the optional part; and
3. The parameters indicted in Table 12/ATIS-1000112.3.

4.11B Long Unitdata Service (LUDTS)

The LUDTS message contains:

1. The label;
2. Four two-octet pointers; and
3. The parameters indicted in Table 12B/ATIS-1000112.3.

4.12 Expedited Data (ED)

The ED message contains:

1. The routing label;
2. One pointer; and
3. The parameters indicated in Table 13/ATIS-1000112.3.

4.13 Expedited Data Acknowledgment (EA)

The EA message contains:

1. The routing label;
2. No pointers; and
3. The parameters indicated in Table 14/ATIS-1000112.3.

4.14 Reset Request (RSR)

The RSR message contains:

1. The routing label;

2. No pointers; and
3. The parameters indicated in Table 15/ATIS-1000112.3.

4.15 Reset Confirmation (RSC)

The RSC message contains:

1. The routing label;
2. No pointers; and
3. The parameters indicated in Table 16/ATIS-1000112.3.

4.16 Protocol Data Unit Error (ERR)

The ERR message contains:

1. The routing label;
2. No pointers; and
3. The parameters indicated in Table 17/ATIS-1000112.3.

4.17 Inactivity Test (IT)

The IT message contains:

1. The routing label;
2. No pointers; and
3. The parameters indicated in Table 18/ATIS-1000112.3.

5 SCCP MANAGEMENT MESSAGES AND CODES

5.1 General

SCCP Management (SCMG) messages are carried using the connectionless service of the SCCP. When transferring SCMG messages, class 0 is requested with the "discard message on error" option. SCCP management message parts are provided in the data parameter of the UDT or XUDT message.

Descriptions of the various parameters are contained in the following clauses. The format of the SCMG message is specified in clause 5.3.

5.1.1 SCMG format identifier

The SCMG format identifier consists of a one-octet field, which is mandatory for all SCMG messages. The SCMG format identifier uniquely defines the function and format of each SCMG message. The allocation of SCMG format identifiers is shown in Table 20/ATIS-1000112.3.

SCMG parameter name codes are given in Table 21/ATIS-1000112.3 with reference to the clauses in which they are described.

5.2 SCMG Message Parameters

5.2.1 End of Optional Parameters

(Deleted, not used in SCMG messages.)

5.2.2 Affected SSN

The affected subsystem number (SSN) consists of one octet coded as directed for the called party address field (see clause 3.4.2.1).

5.2.3 Affected PC

The affected signaling point code (SPC) is represented by three octets that are coded as directed for the called party address field (see clause 3.4.2.2).

5.2.4 Subsystem multiplicity indicator

The subsystem multiplicity indicator parameter consists of one octet coded as shown in Figure 10/ATIS-1000112.3.

The coding of the SMI field is as follows:

bits	21	
	00	affected subsystem multiplicity unknown
	01	affected subsystem is solitary
	10	affected subsystem is duplicated
	11	spare

Bits 3-8 are spare.

5.3 SCMG Messages

SCMG messages are formatted according to the rules given in clause 1.3.

Presently, all SCMG messages contain mandatory fixed parameters only. Each SCMG message contains:

1. Zero pointers; and
2. The parameters indicated in Table 22/ATIS-1000112.3.

Routing Label
Message Type
Mandatory Fixed Part
Mandatory Variable Part
Optional Part

Figure 1/ATIS-1000112.3 - General layout

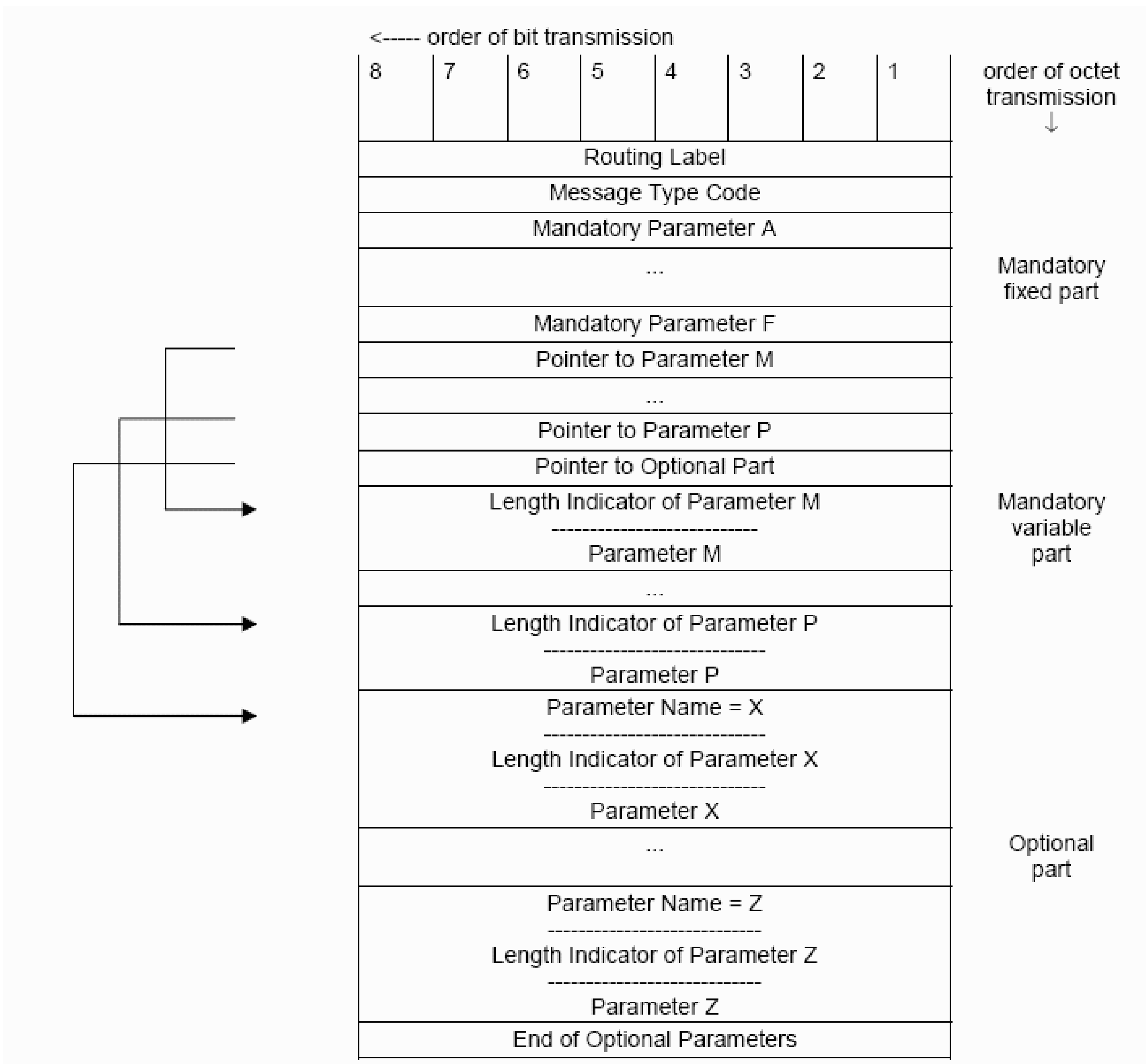


Figure 2/ATIS-1000112.3 - General SCCP Message Format

.	8	7	6	5	4	3	2	1
Octet 1	Address Indicator							
Octet 2 ... Octet n	ADDRESS							

Figure 3/ATIS-1000112.3 - Called, Calling Party Address

8	7	6	5	4	3	2	1
Nat'l Int',l Ind	Rtg Ind	Global Title Indicator				Point Code Ind	SSN Ind

Figure 4/ATIS-1000112.3 - Address indicator encoding[12]

8	7	6	5	4	3	2	1
Subsystem Number							
Signalling Point Code							
Global Title							

Figure 4A/ATIS-1000112.3 - Ordering of Address Elements[4]

8	7	6	5	4	3	2	1
Network Cluster Member							
Network Cluster							
Network Identifier							

Figure 5/ATIS-1000112.3 - Signaling point code encoding

[12] The ordering of the SSN indicator field and the point code indicator field are in a reverse order in the ITU format.

8	7	6	5	4	3	2	1	
Translation Type								octet 1
Numbering Plan				Encoding Scheme				octet 2
Address Information								octet 3 and further

Figure 6/ATIS-1000112.3 - Global title format for indicator 0001[6]

8	7	6	5	4	3	2	1	
Translation Type								octet 1
Address Information								octet 2 and further

Figure 6A/ATIS-1000112.3 - Global title format for indicator 0010

8	7	6	5	4	3	2	1	
2nd address signal				1st address signal				octet 3
4th address signal				3rd address signal				octet 4
...								
filler (if necessary)				nth address signal				octet m

Figure 6B/ATIS-1000112.3 - Global title address information

8	7	6	5	4	3	2	1
reserved							M

Figure 7/ATIS-1000112.3 - Segmenting/reassembling parameter field

8	7	6	5	4	3	2	1
P(R)							/

Figure 8/ATIS-1000112.3 - Receive sequence number

8	7	6	5	4	3	2	1
P(S)							/
P(R)							M

Figure 9/ATIS-1000112.3 - Sequencing/segmenting parameter field

8	7	6	5	4	3	2	1
spare						SMI	

Figure 10/ATIS-1000112.3 - Subsystem Multiplicity Indicator Format

8	7	6	5	4	3	2	1
counter							

Figure 11/ATIS-1000112.3 - SCCP Hop Counter Format

8	7	6	5	4	3	2	1	
F	ISDO	spare		Remaining Segments				Octet 1
Local Reference								Octet 2
								Octet 3
								Octet 4
F="First" bit ISDO=In Sequence Delivery Option								

Figure 12/ATIS-1000112.3 - Segmentation Parameter Format

8	7	6	5	4	3	2	1	
Routing Control								Octet 1
Routing Control Extension								Octet 2t
Network ID 1								Octet 2+t Octet 3+t
Network ID 2								Octet 4+t Octet 5+t
⋮								
Network ID N								Octet 2N+t Octet 2N+t+1

The variable, t, is zero for Type 0 ISNI parameter format, and one for Type 1 ISNI parameter format. Octet 2t is absent and Octet 2+t becomes the second octet when the variable, t, is zero. N is less than or equal to seven.

Figure 13/ATIS-1000112.3 - ISNI Parameter Format

8	7	6	5	4	3	2	1	
Counter			TI	Res	IRI		MI	Octet 1
spare					Network Specific			Octet 2t

Figure 13A/ATIS-1000112.3 - ISNI Routing Control Octets Format

This ISNI routing control octet is coded as follows:

Bits	1	Mark for Identification Indicator (MI)
	0	Do not identify networks.
	1	Identify networks.
Bits	32	ISNI Routing Indicator (IRI)
	00	Neither constrained nor suggested ISNI routing.
	01	Constrained ISNI routing.
	10	Reserved for suggested routing.
	11	Spare
Bits	4	Reserved for expansion of the IRI field.
Bits	5	Type Indicator (TI).
	0	Type zero ISNI parameter format.

	1	Type one ISNI parameter format.
Bits	876	Counter.

Each ISNI Network Identifier (NID) consists of the one-octet Network Identifier followed by the one-octet Cluster Identifier. For large networks, the second octet may be coded all zeroes, or may be coded with the Cluster Identifier of a particular node within the large network. For small networks, two non-zero octets are required to identify the network.

8	7	6	5	4	3	2	1
Counter		Reserved		Type of Routing		Information Type	
Network Identifier 1 (2 octets)							
Network Identifier 2 (2 octets)							

Figure 14/ATIS-1000112.3 – INS Parameter

The INS parameter is coded as follows:

- The third octet is coded as follows:

Bits	12	Information Type Indicator
	00	SS7 format
	01	Reserved
	10	Network-Specific
	11	Network-Specific
Bits	34	Type of Routing
	00	Neither Constrained Nor Suggested INS Routing
	01	Constrained INS Routing
	10	Suggested INS Routing
	11	Reserved
Bits	56	Reserved
Bits	78	Counter

- Octets 4 and 5 Network Identifier 1

Depending on the value of the Information Type, the fourth and fifth octets will be encoded in SS7 format[13] as a combination of "network code" plus "cluster code," or as a two-octet network-specific identifier.

♦ Octet 6 and 7 Network Identifier 2

If present, the sixth and seventh octets will be encoded in SS7 format as a combination of "network codes" plus "cluster codes."

8	7	6	5	4	3	2	1
Reserved for extension	Drop Option	Spare			Original Message Type		

Figure 15/ATIS-1000112.3 – Message Type Interworking Parameter

Bits 1-3 are the Original Message Type field, and it specifies the original message type used before a message change. It is coded as follows:

bits	321	
	000	unqualified
	001	UDT(S)
	010	XUDT(S)
	011	LUDT(S)
	100	spare
	101	spare
	110	spare
	111	spare

Bits 4, 5, 6 are spare.

Bit 7 is the Drop Option field. It indicates whether the Message Type Interworking parameter could be dropped.

bits	7	
	0	Parameter cannot be dropped
	1	Parameter can be dropped

Bit 8 is reserved for extension.

[13] For large networks, the first octet is the NID in the SS7 Point Code (the second octet may be coded with a cluster value or with all zeros); for small networks, two octets are required to identify the network.

Table 1/ATIS-1000112.3 - SCCP Message Types

MESSAGE TYPE	CLASSES				SECT.	MESSAGE TYPE CODE
	0	1	2	3		
CR connection request			X	X	4.2	0000 0001
CC connection confirm			X	X	4.3	0000 0010
CREF connection refused			X	X	4.4	0000 0011
RLSD released			X	X	4.5	0000 0100
RLC release complete			X	X	4.6	0000 0101
DT1 data form 1			X		4.7	0000 0110
DT2 data form 2				X	4.8	0000 0111
AK data acknowledgment				X	4.9	0000 1000
UDT unitdata	X	X			4.10	0000 1001
UDTS unitdata serv.	X	X			4.11	0000 1010
ED expedited data.				X	4.12	0000 1011
EA expedited data ak.				X	4.13	0000 1100
RSR reset request				X	4.14	0000 1101
RSC reset confirmation				X	4.15	0000 1110
ERR error			X	X	4.16	0000 1111
IT inactivity test			X	X	4.17	0001 0000
XUDT extended unitdata	X	X			4.10A	0001 0001
XUDTS ext. unit. serv.	X	X			4.11A	0001 0010
LUDT long unitdata	X	X			4.10B	00010011
LUDTS long unitdata serv	X	X			4.11B	00010100

Table 2/ATIS-1000112.3 - SCCP Parameter Name Codes

PARAMETER NAME	REF.	PARAMETER NAME CODE 8765 4321
End of optional parameters	3.1	0000 0000
Destination Local Reference	3.2	0000 0001
Source Local Reference	3.3	0000 0010
Called Party Address	3.4	0000 0011
Calling Party Address	3.5	0000 0100
Protocol class	3.6	0000 0101
Segmenting/reassembling	3.7	0000 0110
Receive sequence number	3.8	0000 0111
Sequencing/segmenting	3.9	0000 1000
Credit	3.10	0000 1001
Release Cause	3.11	0000 1010
Return Cause (formerly Diagnostic)	3.12	0000 1011
Reset Cause	3.13	0000 1100
Error Cause	3.14	0000 1101
Refusal Cause	3.15	0000 1110
Data	3.16	0000 1111
Segmentation	3.18	0001 0000
SCCP hop counter	3.17	0001 0001
Reserved (used in ITU-T for importance parameter)		0001 0010
Long Data	3.20	0001 0011
Message Type Interworking	3.22	1111 1000
INS	3.21	1111 1001
ISNI	3.19	1111 1010

Table 3/ATIS-1000112.3 - Connection Request Message

Parameter	Reference	Type F V O	Length (octets)
Message Type code	2.1	F	1
Source Local Reference	3.3	F	3
Protocol class	3.6	F	1
Called Party Address	3.4	V	3 min.
Credit	3.10	O	3
Calling Party Address	3.5	O	4 min.
Data	3.16	O	3-130
SCCP hop counter	3.17	O	3
End of optional parameters	3.1	O	1

Table 4/ATIS-1000112.3 - Connection Confirm Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Destination Local Reference	3.2	F	3
Source Local Reference	3.3	F	3
Protocol class	3.6	F	1
Credit	3.10	O	3
Called Party Address	3.4	O	4 min.
Data	3.16	O	3-130
End of optional parameters	3.1	O	1

Table 5/ATIS-1000112.3 - Connection Refused Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Destination Local Reference	3.2	F	3
Refusal Cause	3.15	F	1
Called Party Address	3.4	O	4 min.
Data	3.16	O	3-130
End of optional parameters	3.1	O	1

Table 6/ATIS-1000112.3 - Released Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Destination Local Reference	3.2	F	3
Source Local Reference	3.3	F	3
Release Cause	3.11	F	1
Data	3.16	O	3-130
End of optional parameters	3.1	O	1

Table 7/ATIS-1000112.3 - Release Complete Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Destination Local Reference	3.2	F	3
Source Local Reference	3.3	F	3

Table 8/ATIS-1000112.3 - Data Form 1 Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Destination Local reference	3.2	F	3
Segmenting / Reassembling	3.7	F	1
Data	3.16	V	2-256

Table 9/ATIS-1000112.3 - Data Form 2 Message

Parameter	Reference	Type F V O	Length (octets)
Message type	2.1	F	1
Destination Local Reference	3.2	F	3
Sequencing/Segmenting	3.9	F	2
Data	3.16	V	2-256

Table 10/ATIS-1000112.3 - Data Acknowledgment Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Destination Local Reference	3.2	F	3
Receive Sequence Number	3.8	F	1
Credit	3.10	F	1

Table 11/ATIS-1000112.3 - Unitdata Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Protocol Class	3.6	F	1
Called Party Address	3.4	V	3 min.
Calling Party Address	3.5	V	2 min.
Data	3.16	V	2-252[1]
NOTE 1 - The transfer of up to 252 octets of user data is allowed provided that the maximum length of the SIF as specified in ATIS-1000111.3, clause 2.3.8, is not exceeded.			

Table 11A/ATIS-1000112.3 - Extended Unitdata Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Protocol Class	3.6	F	1
SCCP hop counter	3.17	F	1
Called Party Address	3.4	V	3 min.
Calling Party Address	3.5	V	2 min.
Data	3.16	V	2-251[1]
Segmentation	3.18	O	6
ISNI	3.19	O	3-18
INS	3.21	O	5-7
Message Type Interworking	3.22	O	3
End of optional parameters	3.1	O	1
NOTE 1 - The transfer of up to 251 octets of user data is allowed provided that the maximum length of the SIF as specified in ATIS-1000111.3, clause 2.3.8, is not exceeded.			

Table 11B/ATIS-1000112.3 - Long Unitdata Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Protocol Class	3.6	F	1
SCCP hop counter	3.17	F	1
Called Party Address	3.4	V	3 min.
Calling Party Address	3.5	V	3 min.
Long Data	3.20	V	3-3904[1]
Segmentation	3.18	O	6[2]
ISNI	3.19	O	3-18
INS	3.21	O	5-7
End of optional parameters	3.1	O	1
NOTE 1 - The transfer of up to 3904 octets of user data is allowed, provided that the maximum MTP Signaling Data Unit length is not exceeded as indicated in ATIS-1000111.1. NOTE 2 - Originating SCCP node must include this parameter if segmentation at relay node may be encountered in certain network configurations.			

Table 12/ATIS-1000112.3 - Unitdata Service Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Return cause (formerly Diagnostic)	3.12	F	1
Called Party Address	3.4	V	3 min.
Calling Party Address	3.5	V	2 min.
Data	3.16	V	2-251[1]
NOTE 1 - See NOTE 1 of Table 11/ATIS-1000112.3.			

Table 12A/ATIS-1000112.3 - Extended Unitdata Service Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Return Cause (formerly Diagnostic)	3.12	F	1
SCCP hop counter	3.17	F	1
Called Party Address	3.4	V	3 min.
Calling Party Address	3.5	V	2 min.
Data	3.16	V	2-251[1]
Segmentation	3.18	O	6
INS	3.21	O	5-7
Message Type Interworking	3.22	O	3
ISNI	3.19	O	3-18
End of optional parameters	3.1	O	1
NOTE 1 - See NOTE 1 of Table 11A/ATIS-1000112.3.			

Table 12B/ATIS-1000112.3 - Long Unitdata Service Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Return Cause (formerly Diagnostic)	3.12	F	1
SCCP hop counter	3.17	F	1
Called Party Address	3.4	V	3 min.
Calling Party Address	3.5	V	3 min.
Data	3.16	V	3-3904[1]
Segmentation	3.18	O	6
ISNI	3.19	O	3-18
INS	3.21	O	5-7
End of optional parameters	3.1	O	1
NOTE 1 - See NOTE 1 of Table 11B/ATIS-1000112.3.			

Table 13/ATIS-1000112.3 - Expedited Data Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Destination Local Reference	3.2	F	3
Data	3.16	V	2-33

Table 14/ATIS-1000112.3 - Expedited Data Acknowledgment Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Destination Local Reference	3.2	F	3

Table 15/ATIS-1000112.3 - Reset Request Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Destination Local Reference	3.2	F	3
Source Local Reference	3.3	F	3
Reset Cause	3.13	F	1

Table 16/ATIS-1000112.3 - Reset Confirmation Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Destination Local Reference	3.2	F	3
Source Local Reference	3.3	F	3

Table 17/ATIS-1000112.3 - Error Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Destination Local Reference	3.2	F	3
Error Cause	3.14	F	1

Table 18/ATIS-1000112.3 - Inactivity Test Message

Parameter	Reference	Type F V O	Length (octets)
Message Type	2.1	F	1
Destination Local Reference	3.2	F	3
Source Local Reference	3.3	F	3
Protocol Class	3.6	F	1
Sequencing/segmenting[1]	3.9	F	2
Credit[1]	3.10	F	1
NOTE 1 - Information in these parameter fields reflects those values sent in the last Data Form 2 or Data Acknowledgment message. They are ignored if the protocol class parameter indicates Class 2.			

Table 19/ATIS-1000112.3 - SCCP Management Message Format

Parameter	Reference	Type F V O	Length (octets)
Message Type (= Unitdata)	2.1	F	1
Protocol Class (= Class 0, no return)	3.6	F	1
Called Party Address (SSN = SCCP Management)	3.4	V	3
Calling Party Address (SSN = SCCP Management)	3.5	V	3
Data (Data consists of an SCMG message with format as in Table 22/ATIS-1000112.3)	3.16	V	7

Table 20/ATIS-1000112.3 - SCMG Format Identifiers

MESSAGE	CODE 8765 4321
SSA Subsystem-allowed	00000001
SSP Subsystem-prohibited	00000010
SST Subsystem-status-test	00000011
SOR Subsystem-out-of-service-request	00000100
SOG Subsystem-out-of-service-grant	00000101
Reserved (Used in ITU-T for SSC message)	00000110
SBR Subsystem-backup-routing	11111101
SNR Subsystem-normal-routing	11111110
SRT Subsystem-routing-status-test	11111111

Table 21/ATIS-1000112.3 - SCMG Parameter Name Codes

PARAMETER NAME	REF.	PARAMETER NAME CODE 8765 4321
Affected SSN	5.2.2	0000 0001
Affected PC	5.2.3	0000 0010
Subsystem Multiplicity Indicator	5.2.4	0000 0011

Table 22/ATIS-1000112.3 - SCMG Message

Parameter	Reference	Type F V O	Length (octets)
SCMG format identifier (Message type code)	5.1.1	F	1
Affected SSN	5.2.2	F	1
Affected PC	5.2.3	F	3
Subsystem Multiplicity Indicator	5.2.4	F	1

Annex A

(normative)

ANNEX A GUIDELINES AND PROCEDURES FOR ASSIGNING INTERNETWORK TRANSLATION TYPE CODE VALUES

A.1 Introduction

This Annex contains the criteria and guidelines for the assignment of Translation Type code values to be used by the United States CCS networks for internetwork messaging. In addition, this Annex contains the procedures for requesting an internetwork Translation Type code value, and a list of the assigned code values. It is assumed that other North American CCS networks will follow the same guidelines and procedures as United States CCS networks.

In order to assign a Translation Type for a particular application, the following conditions must be met:

1. The application must require internetwork messaging;
2. It has been determined that the application cannot fit into a previously defined application/translation group, and hence requires a new Translation Type code value;
3. A proposal for an internetwork Translation Type has been brought to T1 which:

Includes a high level description of the application; and

Defines the application's translation needs.

When a new application that fits into a previously defined application/translation group is being defined (i.e., the new application would use an already assigned translation type value), the organization defining the new application is responsible for proposing appropriate modifications to the existing application/translation group description in Annex B.

A.2 Assumptions

The following assumptions have been made:

1. These guidelines and procedures apply to translation types in the internetwork range only. The usage of translation types in the network specific range is not affected.
2. A particular value for an internetwork Translation Type in conjunction with the Global Title value are always sufficient information to determine the destination application (Destination Point Code and Subsystem Number) in the *terminating network*. This does not preclude multiple global title translations.
3. No assumptions are made on the use of Translation Type for Global Title Indicator 0001. Use of global titles with numbering plan and encoding scheme is left for further study, pending more information on how these would actually be used by networks.

A.3 Definitions

The following terms are defined in this Annex to prevent confusion with other possible definitions:

1. *Global Title* - An alias address for an application which is composed of digits; translation of this alias will result in at least a point code; note that this point code can be that of a Signaling Transfer Point (STP), a switch, a Service Control Point (SCP), or some other signaling point. (Clause 2.1 of ATIS-1000112.4 defines the Global Title as the following: *an address, such as dialed digits, that does not explicitly contain information that would allow routing in the signaling network.*)

2. *Global Title Translation* - The process by which a Global Title is translated into a combination of one or more of the following: a point code, subsystem number, and Global Title.

3. *Translation Type* - Directs a message to the appropriate Global Title Translation function; and in some cases it provides the context under which the Global Title digits are to be interpreted.

4. *Translation needs* - Describe the input and output of a Global Title Translation function. Some requirements can be given on the allowed format and the minimum information (minimum number of digits, for example) that must be provided.

5. *Application* - The module of processing that can originate and receive a non-circuit-related signaling message. An example might be the application that provides "busy/idle line status," which, when queried, returns the status of an identified line. A given service may involve the use of multiple applications. "Application" is used here independently of the pure OSI definition for application layer protocol.

6. *Application/Translation group* - A set of applications which can be grouped together because of the following characteristics:

   a. All members of the group have a single set of translation needs, i.e., for a given Global Title value, the same Destination Point Code and Subsystem Number will result after translation (the context of the message itself determines the specific application within the group required at the node).

   b. If this set of applications is implemented at a single node the following would be true:

      - Messages received at the terminating node for the group can be processed without needing the SCCP to identify which specific application should do the processing (i.e., a single subsystem number can be used to address all applications within the group.)

      - There are no TCAP coding conflicts or ambiguities with applications in the application group

      - The applications within the group do not need to be individually distinguished for subsystem management (i.e., individual applications do not need to be able to fail independently or need their status to be maintained independently).

   Note that a group may consist of a single member, and that one application may belong to multiple groups, based on multiple translation needs.

7. *Subsystem management/functions* - (from ATIS-1000112.4, clause 5.1) The purpose of SCCP management is to provide procedures to maintain network performance by rerouting or throttling traffic in the event of failure or congestion in the network. (This definition is provided to define the subsystem management procedures mentioned above in the discussion of *application/translation group.*)

8. *Internetwork messaging* - Messages that traverse at least one network boundary.

A.4 Guidelines for Assigning Internetwork Translation Type Code Values

A.4.1 Constraints and Logistics

1. Only Translation Type codes in the internetwork range can be assigned.
2. At most one Translation Type code can be assigned to an application/translation group.
3. In order to assign a Translation Type for a particular application/translation group, the application/translation group must at minimum currently require or in the future require internetwork messaging.

A.4.2 Determining Translation Type Needs

When the Stage 3 of an application is defined which uses a TCAP protocol element, it is necessary to determine if:

1. The application fits into a previously defined application/translation group which has an assigned Translation Type;
2. A new application/translation group (with a new Translation Type) must be defined; or
3. There is no need for a Translation Type to be assigned for this application.

Non-standardized applications follow a similar procedure.

A.4.3 Determining the Application/Translation Group

An application/translation group must be described in terms of:

1. The translation needs.
2. A high-level description of each application currently in the application/translation group; this does not preclude future applications from being added to the application/translation group. These descriptions should be from the perspective of a TCAP user.

   NOTE - Applications need not be *standardized* applications in order to use internetwork Translation Types, nor do the Stage 1 descriptions have to be standardized. The Stage 1 descriptions are for discussion purposes and to describe the application that will be using a particular Translation Type.

3. It is possible to have only one application in an application/translation group.

A.5 Procedures for Requesting a Translation Type Code Assignment

Initially, it must be determined if a code assignment should be made. If so, either a new application/translation group is being defined, or a new application will be included into an existing application/translation group.

A.5.1 Content of Proposal

In order to assign a Translation Type for a new application/translation group or to insert a new application into an existing application/translation group, a proposal must be submitted to Committee T1. The content of this proposal is described below.

1. *Application Description*: The new application/translation group or the new application should be described in a high level fashion. This statement must unambiguously describe the new application/translation group.
2. *Internetwork Needs*: The statement must explain why the new application/translation group or application requires internetwork messaging currently or in the near future.
3. *Involved Nodes*: It is assumed that the new application or new application/translation group will, at some point, require Global Title Translations for proper application execution. An example of the terminating and originating nodes should be listed (i.e., Stored Program Control Switching Systems, Service Control Points, etc.). A reference diagram showing the node configuration would be helpful.
4. *Global Title Translation Requirements*: The basic format of the input and output of the Global Title Translation (GTT) must be delineated. This information includes the numbering plan, encoding scheme, and number of digits (e.g., "5" or "6-10") of the input to GTT and the expected output.

   NOTE - The identity of the application is not determined from the digits in the global title, but from the translation type.
5. *Relationship to Existing Application/Translation Groups*: If the translation needs are similar to any existing application/translation groups, the relationship to these groups should be explained. If a new application/translation group is proposed, this should be justified, e.g., by:
   - *New TCAP encoding needs* - Encoding of the TCAP protocol elements such as operation codes, error codes or parameters will conflict with that in existing groups (i.e., different application context).
   - *New resource/management needs* - The application requires that resources be independently allocated and managed from existing groups.

A.5.2 Assignment of Translation Type Codes

Translation Type codes for internetwork applications will be assigned in ascending order starting with "00000001." The assignment of Translation Type codes should be as described in Table A-1/ATIS-1000112.3. Network providers should continue to use network specific Translation Types as they see fit.[14] A descending order of assignment is recommended for network specific values.

Network providers may initially implement services within the network specific range. If a particular service evolves to the point that it requires an internetwork value assignment, the network providers must use, at the interface, the assigned internetwork value.

[14] Assignment of internetwork values does not imply that network specific translation types cannot be used between networks.

Table A-1/ATIS-1000112.3 - List of Translation Type Code Values

Translation Type Code Values		
Decimal	Bits 87654321	Application/Translation Group
0	00000000	reserved
1	00000001	Identification Cards
2	00000010	reserved - see Note 1
3	00000011	Cellular Nationwide Roaming Service
4	00000100	Global Title = Point Code
5	00000101	Calling Name Delivery
6	00000110	reserved - see Note 1
7	00000111	Message Waiting
8	00001000	SCP Assisted Call Processing
9	00001001	National and International Cellular/PCS Roaming
10	00001010	Network Entity Addressing
11	00001011	Internetwork NP Query/Response (NP Q/R)
12	00001100	Wireless MIN-Based Short Message Service
13	00001101	Wireless IMSI-Based Short Message Service
14	00001110	Mobile Subscriber Addressing
15	00001111	Packet Data Interworking
16	00010000	Cellular/PCS Interworking
17	00010001	Mobile Subscriber Message Center Addressing
18	00010010	ECS Call Routing
19 27	00010011 to 00011011	inter-network applications
28	00011100	14 Digit Telecommunication Calling Cards – Post-10-digit (NP) GTT (see Note 3)
29	00011101	Calling Name Delivery – Post-10-digit (NP) GTT (see Note 3)
30	00011110	Call Management – Post-10-digit (NP) GTT (see Note 3)
31	00011111	Message Waiting – Post-10-digit (NP) GTT (see Note 3)
32 191	00100000 to 10111111	spare
192 249	11000000 to 11111001	network specific applications
250	11111010	network specific applications
251	11111011	reserved - see Note 1
252	11111100	network specific applications
253	11111101	reserved - see Note 1
254	11111110	see Note 2
255	11111111	reserved

NOTE 1 - Due to historical technical limitations in equipment, the value 253 has been used for both the 14 Digit Calling Card application and network specific applications, and the value 251 has been used for both the Call Management application and other network specific applications. Therefore, either 2 or 253, or 6 or 251, may be selected for the 14 Digit Calling Card application or Call Management application, respectively. Special bilateral discussions should be held to determine the best arrangement to facilitate interworking of the Translation Types to support these applications at each interface. The use of 251 and 253 for network specific applications is not precluded. No use of any other network specific values for internetwork applications will be considered.

NOTE 2 - The network specific value "254" is already in use by some network providers for internetwork applications (for example, 800 Service.) Network providers who have not implemented this value are advised to consider the potential translation type code conflicts of its use for network specific applications.

NOTE 3 - This assignment is made for purposes of loop detection and prevention anticipating that future loop detection and prevention mechanisms (e.g., use of the XUDT Hop Counter) may support the return of these values to the translation type assignment pool.

GENERAL NOTE - An application/translation group may be described using a particular technology (e.g., PCS or Cellular). However, this does not normally imply that the use of the translation type is restricted to a particular technology, type of network or organization. If the routing needs of an application/translation group may be technology dependent, the use of Global Title Address Information (GTAI) should be investigated to convey technology specific information.

Annex B
(informative)

ANNEX B DESCRIPTIONS OF APPLICATION/TRANSLATION GROUPS

This informative Annex describes the application/translation groups that have been assigned internetwork translation type values as listed in Table A-1/ATIS-1000112.3. Each application/translation group is described (as defined in ATIS-1000112.3/A.5.1) in terms of:

- ♦ Application description
- ♦ Internetwork needs
- ♦ Involved nodes
- ♦ Global title translation requirements
- ♦ Relationship to existing application/translation groups.

B.1 TRANSLATION TYPE CODE VALUE: 00000001 (1)

Application/Translation Group: *Identification Cards*

B.1.1 Application Description

Identification cards as described in ISO/7812, *Identification card - numbering system and registration procedure for issuer identifiers*, include airlines, travel and entertainment, banking/financial, merchandizing and banking, petroleum, and telecommunications applications.

The Identification Cards application/translation group includes the following applications:

- ♦ *891 Telecommunication Charge Card Application* - The 891 telecommunication credit cards are used for payment of telephone charges and service charges, and validation procedures. The 891 Telecommunication Charge Card has been approved by ATIS [T1.212-1995 (R1999)] based on ITU-T Recommendation E.118 (Automated International Telephone Credit Card System) and ITU-T Recommendation E.164 (Numbering Plan for the ISDN Era). Network providers of these cards may arrange for a consistent Translation Type with all other network providers of these cards.
- ♦ *Banking/Financial Calling Card Application* - The banking/financial calling cards are used for payment of telephone and service charges through a calling card provider. They will also be used for validation procedures to a centralized Record Information Database (RIDB). This application will allow customers to use their existing commercial credit cards with a uniquely assigned Personal Identification Number (PIN) for charging telephone calls. The Banking/Financial Calling Card Application is being established so that providers of the card may arrange with network service providers for consistent routing of telecommunications messages. The Banking/Financial Calling Card is based on an ISO/7812 superset of ITU-T Recommendation E.118.

B.1.2 Internetwork Needs

When the Identification Cards are used outside of the card issuing network, then internetwork messaging occurs and an internetwork Translation Type is required.

B.1.3 Involved Nodes

The Identification Card applications use an Operator Services signaling point as its originating signaling point and involves Global Title Translation at one or more Signaling Transfer Points (STPs) and terminates in an Identification Card database (e.g., 891 database, RIDB).

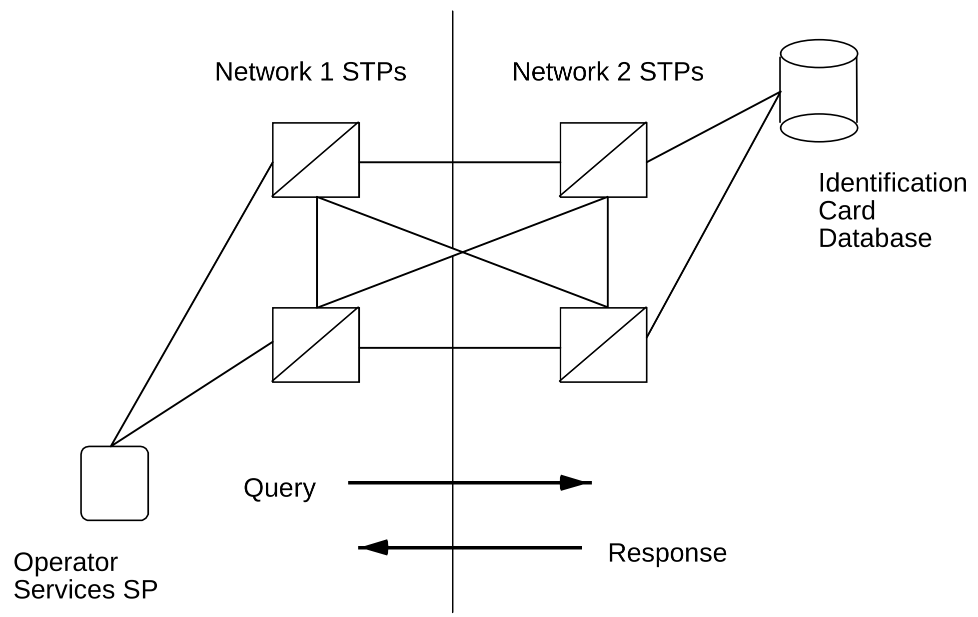


Figure B-1/ATIS-1000112.3 - Identification Card Example Diagram

B.1.4 Global Title Translation Requirements

B.1.4.1 Format of Identification Card (as described in ISO/IEC 7812 - 1)

A BCDEF GHIJKLMNOPQR S

A - Major Industry Identifier (MII)

The major industry identifier is assigned as follows:

0 - for assignment by ISO-TC68 and for other future industry

1 - airlines

2 - airlines and other future industry assignments

3 - travel and entertainment

4 - banking/financial (see clause 2.4.1)

5 - banking/financial (see clause 2.4.1)

6 - merchandizing and banking

7 - petroleum

8 - telecommunications and other future industry assignments (see clause 2.4.2)

9 - for assignment by national standards bodies

BCDEF - Issuer Identifier (fixed length - 5 digits)

Note that the Issuer Identification Number (IIN) consists of the MII together with the Issuer Identifier (i.e., ABCDEF)

GHIJKLMNOPQR - Individual Account Identification Number (variable - maximum 12 digits)

S - Check Digit

B.1.4.2 Format of Banking/Financial Calling Card

A BCDEF GHIJKLKLMNOPQR S TUVW

A - Major Industry Identifier (MII) is 4 or 5

BCDEF GHIJKLMNOPQR S - same as standard Identification Card above

TUVW - Personal Identification Number (4 digits - not visible)

* Issuer Identification Numbers beginning with "59" are issued by financial institutions and not by the Registration Authority under ISO/IEC 7812. These cards are not addressed by this application/translation group.

B.1.4.3 Format for 891 Telecommunication Charge Card (for World Zone 1)

AB CDE FGHIJKLMNOPQRS - Primary Account Number

A - Major Industry Identifier (MII) is 8

AB - 89 is assigned for telecommunication purposes**

C - Country Code ITU-T E.164 (variable 1-3 digits, 1 digit for World Zone 1)

DEF - Issuer Identifier (variable 1-4 digits, 3 digits for World Zone 1)

ABCDEF - Issuer Identification Number (IIN) (variable - max 7, 6 digits for World Zone 1)

GHIJKLMNOPQR - Individual Account Identification Number (variable 1-14 digits, but fixed for each particular IIN)

S - Check Digit

** Issuer Identification Numbers beginning with "89" are used on cards issued by telecommunications administrations and recognized private operating agencies in accordance with ITU-T Recommendation E.118. These IINs are maintained by the International Telecommunication Union.

B.1.4.4 Global Title Translation Addressing Information

The global title address information contains at least the first 6 digits of the identification number.

For the Banking/Financial Calling Card Application, the global title address contains the MII and the Issuer Identifier with the format "ABCDEF" as shown above.

For the 891 Telecommunication Charge Card Application, the global title address contains the MII, the country code, and the Issuer Identifier as shown above.

It is expected that 6 digits of the global title address information will be used for global title translation (GTT). This address information is encoded as binary-coded-decimal (BCD). Global Title Indicator type 2 will be used. The output of the final GTT will be the point code and SSN of the Identification Card database.

B.1.5 Relationship to Existing Application/Translation Groups

These applications are similar to 14 digit telecommunications calling card, however, translation requirements differ from those for the 14 digit calling card. Independent resources and management are needed, as well.

The encoding of the TCAP operation codes, parameters, and error codes for the 891 Telecommunication Charge Card Application and the Banking/Financial Calling Card application will not conflict, due to the global title addressing scheme.

NOTE 1 - For 891 telecommunications credit card applications, this application group is for the use of World Zone 1 to World Zone 1 calls within the United States. No statement is made as to its applicability outside of the area covered by T1.

NOTE 2 - The use of 891 cards outside of the United States is for further study.

NOTE 3 - The use of 89x cards as a generic contribution is for further study.

B.1.6 ISO Standards

ISO/7819, *Identification cards - Physical characteristics*.[15]

ISO/7811/1, *Identification cards - Recording technique - Part 1: Embossing*.[15]

ISO/7811/2, *Identification cards - Recording technique - Part 2: Magnetic stripe*.[15]

ISO/7811/3, *Identification cards - Recording technique - Part 3: Location of embossed characters*.[15]

ISO/7811/4, *Identification cards - Recording technique - Part 4: Location of read-only magnetic tracks - Tracks 1 and 2*.[15]

ISO/7811/5, *Identification cards - Recording technique - Part 5: Location of read-write magnetic track - Track 3*.[15]

ISO/7812/1, *Identification cards - Identification of Issuer - Part 1: Numbering System*.[15]

---

[15] This document is available from the International Organization for Standardization. < http://www.iso.ch/iso/en/prods-services/ISOstore/store.html >

ISO/7812/2, *Identification cards - Identification of Issuer - Part 2: Application and registration procedures*.[15]

ISO/7813, *Identification cards - Financial transaction cards T& l s*.[15]

NOTE - The standard for the IC card is to be established by ISO TC 97/SC 17/W G 4.

B.2 TRANSLATION TYPE CODE VALUE: 00000010 (2), 11111011 (253)

Application/Translation Group *14 Digit Telecommunications Calling Cards*

B.2.1 Application Description

The 14 Digit Format Telecommunications Calling Card Application is being established so that network providers of these cards may arrange for a consistent Translation Type with all other network providers of these cards. The 14 Digit Format Telecommunications Calling Card has been provided by ITU Recommendation E.113, *Procedures for an Automatic International Telephone Credit Card System*.[16]

The 14 Digit Format Telecommunications Calling Card will be used for:

- Payment of the telephone charge;
- Service charges due; and
- Validation procedures

to a 14 digit format telecommunications calling card database. This service requires a different database than the 891 telecommunications calling card database.

B.2.2 Internetwork Needs

When the 14 Digit Format Telecommunications Calling Card is used outside of its card issuing network, then internetwork messaging occurs.

B.2.3 Involved Nodes

The 14 Digit Format Telecommunications Calling Card Application uses the Operator Services signaling point as its originating signaling point and terminates in a 14 digit format database (see Figure B-2).

---

[16] This document is available from the International Telecommunications Union.
< http://www.itu.int/ITU-T/ >

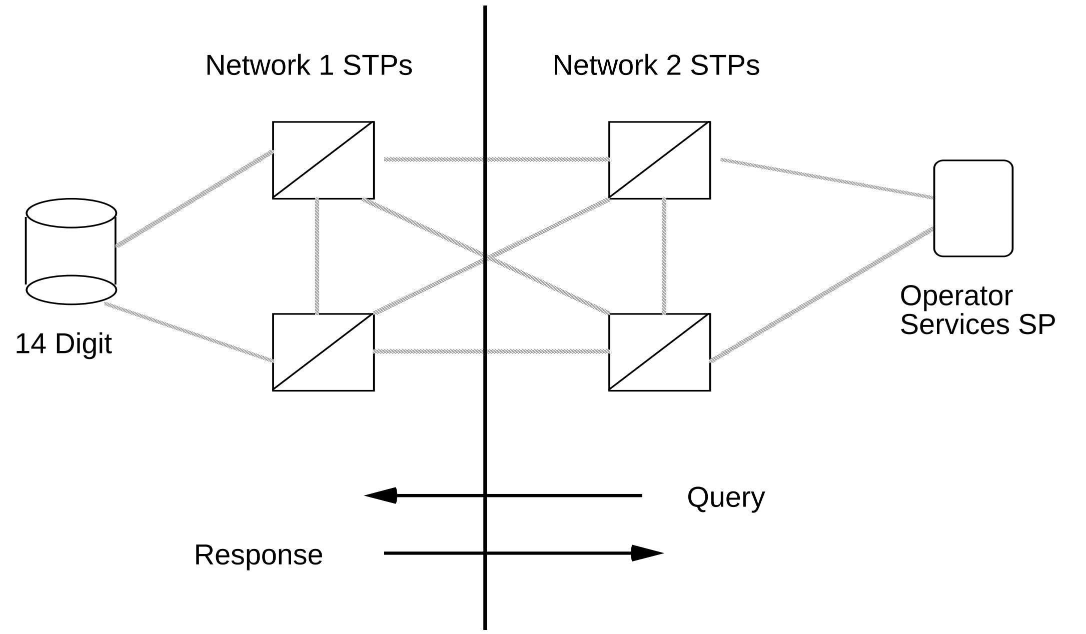


Figure B-2/ATIS-1000112.3 - 14-Digit Telecommunications Calling Card Example Diagram

B.2.4 Global Title Translation Requirements

B.2.4.1 Format of 14 Digit Telecommunications Calling Card

Format: NPA NXX XXXX XXXX where:

- NPA is a valid NPA approved by the North American Number Plan Administrator.
- N can be any digit from 2 - 9
- X can be any digit from 0 - 9

Special Billing Format:

CIID: NXXWXX XXXX NXXX where:

- N can be any digit from 2 - 9
- X can be any digit from 0 - 9
- W can be any digit from 0 - 1; and
- NXXWXX is the card issuer id
- XXXX is the customer account
- NXXX is the personal identification number (non-visible)

RAO: XXX XXXXXXXXXXX where:

- X can be any digit from 0 - 9; and
- XXX is the RAO
- XXXXXXXXXXX is the customer identification number

B.2.4.2 Global Title Translation Addressing Information

The global title address information contains the first 6 or 10 digits of the 14 Digit Telecommunications Calling Card. This address information is encoded as BCD. Global Title Indicator type 2 will be used.

It is expected that the first 3, 6 or 10 digits of the global title address information will be used to perform the GTT. The output of the final GTT will be the point code and SSN of the 14 Digit Calling Card database.

B.2.5 Relationship to Existing Application/Translation Groups

This application is similar to the 891 Telecommunications Calling Card Application Group, but translation requirements are different. Independent resources and management are needed, as well.

B.3 TRANSLATION TYPE CODE VALUE: 00000011 (3)

Application/Translation Group: *Cellular Nationwide Roaming Service*

B.3.1 Application Description

Cellular Nationwide Roaming Service allows a cellular subscriber to request and receive subscribed services while roaming in any system other than the home system. One key procedure to the successful offering of this service is the registration. A cellular terminal passes information such as the Mobile Identification Number (MIN) over the radio interface to the visited system when it registers itself to the system or when the roamer initiates a call or service request. The cellular industry uses the MIN as the global title to route a Registration Notification INVOKE message, a TIA IS-41 Mobile Application Part (MAP) message, from the visited system to the roamer's Home Location Register (HLR)[17] over the interconnecting SS7 networks. Using the GTT capability of the SS7 networks frees the cellular systems from performing GTT-like translation (e.g., mapping the MIN to an SS7 point code and SSN). The roamer's validation qualifications and service profile is retrieved from the HLR and used to determine whether a requested service should be granted.

When the home system receives a call destined toward the roamer, it will interrogate with the visited system for a Temporary Local Directory Number (TLDN) for this call. The TLDN is then used by the Public Switched Telephone Network (PSTN) to route the call to the visited system and by the visited system to associate this incoming call with a specific roamer.

B.3.2 Internetwork Needs

The transport of the Registration Notification INVOKE message will normally involve the Visited Location Register (VLR)[18] in the visited cellular system, HLR in the home cellular system and the interconnecting SS7 network(s). Figure B3 shows the nodes and systems involved in the message transport between the visited and home cellular systems. The VLR in the visited system sends out the

---

[17] The HLR is the location register that stores information for handling calls to and from a home subscriber.

[18] The VLR is the location register that stores information for handling calls to and from a visiting subscriber.

Registration Notification INVOKE message to the interconnecting SS7 network when it is first notified of the presence of a particular roamer. The MIN is used as the global title address information in the SCCP Called Party Address field.

The interconnecting SS7 network then performs the GTT and translates the GT (the MIN) into an SS7 point code and SSN for the HLR. Several STPs in the interconnecting SS7 network may be involved in the message routing. One of them performs the final GTT, which translates the global title into an SS7 point code and SSN.

When the HLR receives the Registration Notification INVOKE message, it will update the current location of the indicated roamer and responds with the roamer's validation requirements and service profile if so requested. The response message is routed back to the VLR in the visited system through the interconnecting SS7 network by MTP routing. If the roamer is previously registered with another system, the HLR will inform that system that the indicated roamer has left its system (not shown in Figure B-3).

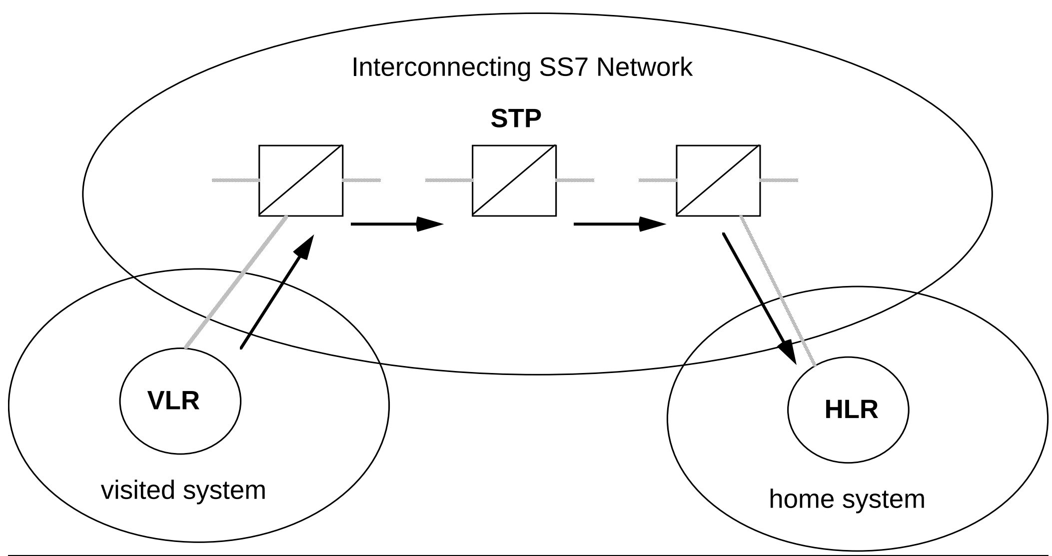


Figure B-3/ATIS-1000112.3 - Involved Nodes When Routing Registration Notification INVOKE Message from the Visited System to the Home System

B.3.4 Global Title Translation Requirements

The global title address information contains the MIN, which is a ten-digit North American Number Plan number with the format of NPA+NXX+XXXX. The numbering plan is ISDN Numbering Plan (ITU-T Rec. E.164) and only the national number portion is used as the global title address. The encoding scheme is BCD. Each address signal is coded is described in clause 3.4.2.3.1 of ATIS-1000112.3. Global Title Indicator type 2 will be used.

It is expected that only 6 to 9 out of the 10 digits of the global title address information will be used to perform the GTT. The output of the final GTT will be the point code and SSN of the HLR.

B.3.5 Relationship to Existing Application/Translation Groups

The IS-41 MAP uses the ANSI TCAP Component and Translation Sub-layer facilities to communicate. The IS-41 MAP uses private operation codes, private error codes, and context-specific parameters identifiers; therefore, its usage of the TCAP does not impact other application/translation groups. The application procedures of the Cellular Nationwide Roaming Service are described in the TIA IS-41 document.

Existing application/translation groups remain unaffected with respect to the new resource/management needs for this application/translation group.

B.4 TRANSLATION TYPE CODE VALUE: 00000100 (4)

Application/Translation Group: *Global Title Address = Point Code*

B.4.1 Application Description

In the development of the procedures for the Intermediate Signaling Network Identification (ISNI) capability, a need has been identified for routing based on a unique form of Global Title. This unique Global Title is one that includes a Translation Type and a Global Title address in the form of a SS7 point code. For ISNI purposes, this type of Global Title would be used when routing SCCP Extended Unitdata (XUDT) response messages and Extended Unitdata Service (XUDTS) messages. In both cases, the point code from the SCCP Calling Party Address of the received message would be used as the Global Title Address "digits" in the transmitted XUDT or XUDTS message. The purpose of this type of routing is to allow intermediate network processing (ISNI routing and/or identification) at the SCCP level to take place.

ISNI is the only application identified at present that would make use of the new Translation Type. However, there may be other applications in the future that require routing based on a Global Title address that is a point code. Only one internetwork Translation Type is required for messages of this type.

B.4.2 Internetwork Needs

The ISNI capability allows an application process in the origination network to select intermediate signaling network(s) for non-circuit associated signaling messages and/or to notify an application process in the destination network about such intermediate signaling network(s). ISNI may be invoked by a variety of services that require internetwork messaging.

B.4.3 Involved Nodes

The single selection scenario for intermediate network routing is shown in Figure B-4. In this scenario, the origination network requires the use of a Signaling End Point (SEP) and possibly the use of STPs. The destination network includes a SEP and STPs. An intermediate network may require the use of STPs only.

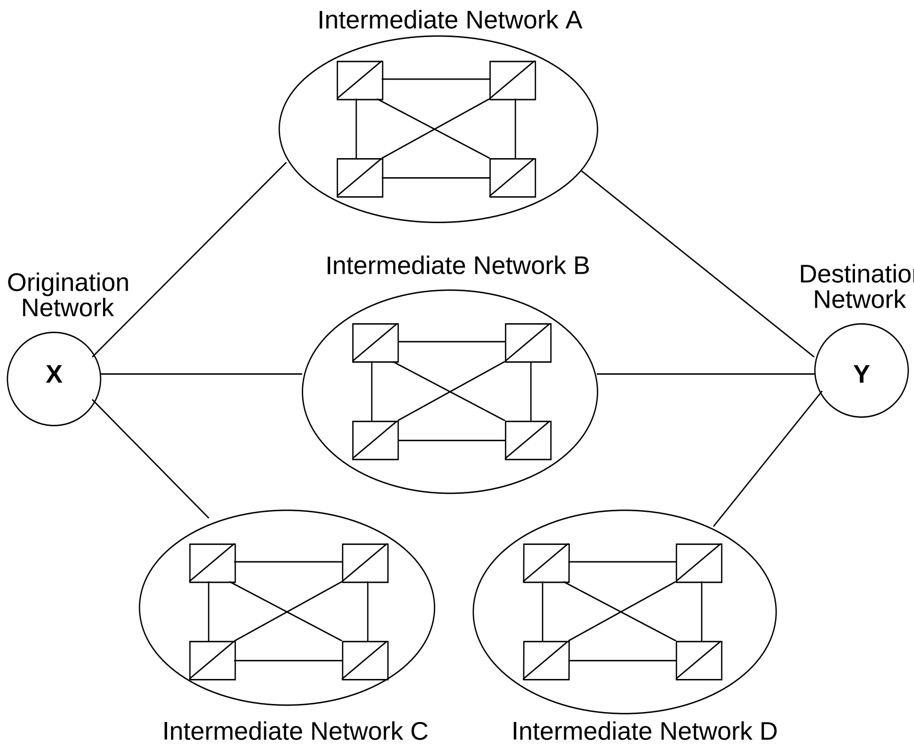


Figure B-4/ATIS-1000112.3 - Single Selection Scenario for Intermediate Network Routing

B.4.4 Global Title Translation Requirements

The basic input and output of the GTT process are shown in Figure B-5 as follows:

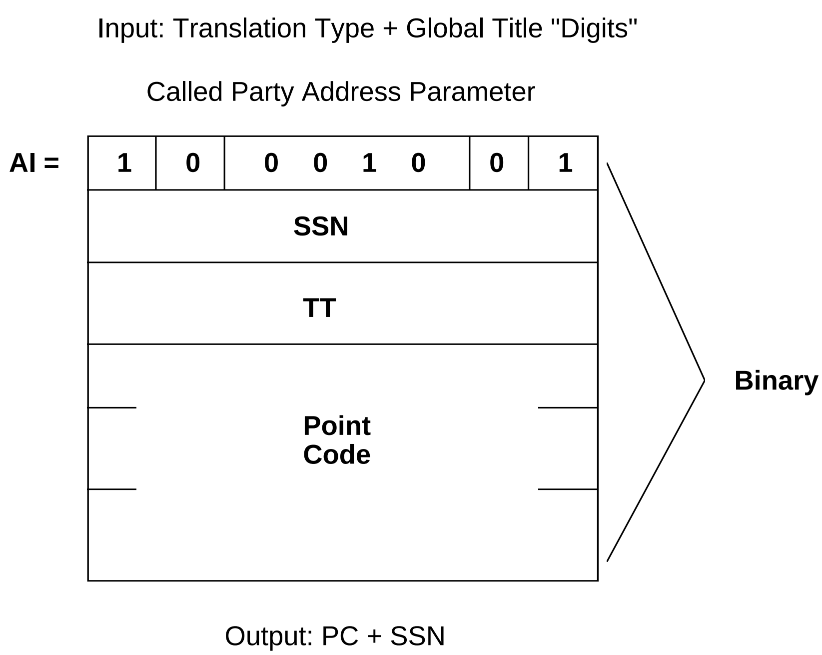


Figure B-5/ATIS-1000112.3 - Format of Called Party Address Parameters for Translation Type = 4

By assigning a unique internetwork Translation Type to Global Title addresses of this type, the GTT process can be simplified greatly. Instead of going through the usual process of mapping the Global Title to a particular output, the SCCP will only need to pass the point code present in the Global Title address field to the MTP for routing. The Global Title Address is composed of three binary octets.

This format does not require the use of a new Global Title Indicator (i.e., Global Title Indicator type 2 will be used) and the point code present in the parameter is part of the Global Title field. Therefore, the point code indicator field in the Address Indicator (AI) octet should be set to zero as normal. The SSN, in this case, is an actual SSN and not the null value.

B.4.5 Relationship to Existing Application/Translation Groups

Existing application/translation groups remain unaffected with respect to the needs for the ISNI application/translation group.

B.5 TRANSLATION TYPE CODE VALUE: 00000101 (5)

Application/Translation Group: *Calling Name Delivery*

B.5.1 Application Description

Calling Name Delivery (CNAM) is a new feature that enables the called subscriber to view the calling party's name on a separately provided display device before the call is answered. The Plain Old Telephone Service (POTS) application of the CNAM service may utilize a name database located at one or more network nodes. In this case, Calling Name information is retrieved from the database by the CNAM subscriber's serving switch via Transaction Capabilities Application Part (TCAP) messages. GTTs are performed at one or more STPs to identify the network node that contains the CNAM information for this particular calling party.

B.5.2 Internetwork Needs

In the future, when a calling party in one network calls a CNAM subscriber in another network, internetwork messaging will occur during the retrieval of the calling party name information from the calling party's associated database. For this reason, an internetwork Translation Type code value is required.

B.5.3 Involved Nodes

The SEP serving the CNAM subscriber generates a TCAP query message that requires GTT routing at one or more STPs. This query message is ultimately routed to the Calling Name database associated with the calling party. Figure B-6 is a Calling Name Delivery example diagram.

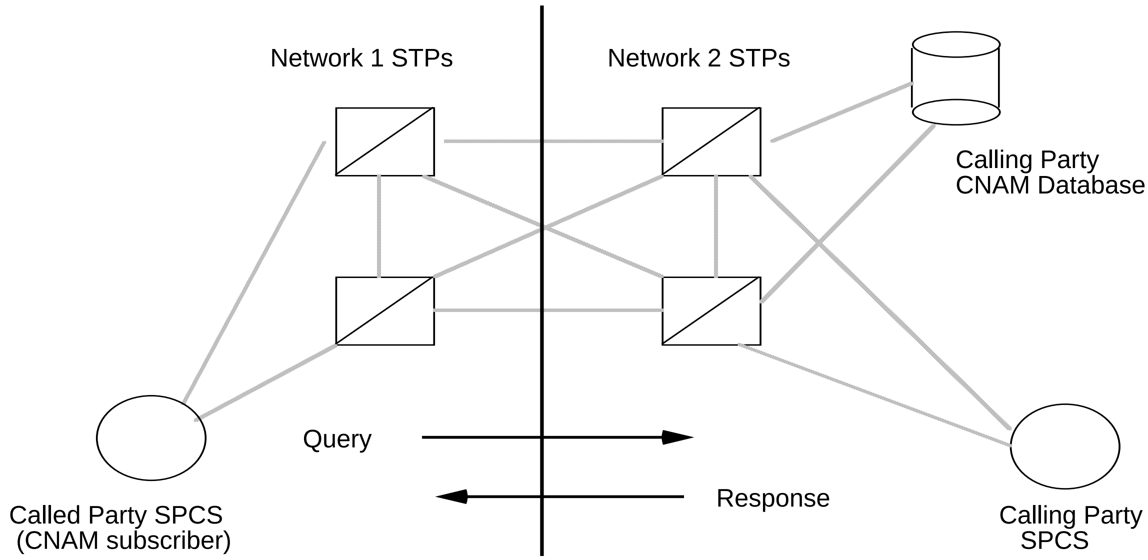


Figure B-6/ATIS-1000112.3 - Calling Name Delivery Example Diagram

B.5.4 Global Title Translation Requirements

The global title address information contains the ten-digit North American Numbering Plan calling party number in the format of NPA+NXX+XXXX. This address information is encoded as BCD. Global Title Indicator type 2 will be used.

It is expected that either 3 or 6-10 digits of the Global Title Address information will be used for GTT. The output of the final GTT will be the point code and SSN of the database where calling name information is stored.

B.5.5 Relationship to Existing Application/Translation Groups

The Global Title Address information in this application/translation group is the same as in other existing groups; however, this application requires independently allocated resources and management (i.e., the output of the global title translation must be the CNAM database).

B.6 TRANSLATION TYPE CODE VALUE: 00000110 (6), 11111011 (251)

Application/Translation Group: *Call Management*

B.6.1 Application Description

Call Management Services are a set of features that utilize the capability to forward a calling party's number between end offices with the Common Channel Signaling (CCS) call setup messages. Call Management services also include applications that use the TCAP layer of the protocol. GTTs may be required at one or more STPs to identify the network node that serves the Called Party. Two examples of Call Management services are Automatic Callback and Automatic Recall.

- *Automatic Callback* is an outgoing call management feature that allows a customer to place a call to the last station called by the customer. The customer places this call by activating a procedure to have call setup performed automatically when the busy called station becomes idle. When activation is completed, the busy/idle status and class of service of the called line are checked. If the line is idle and the class of service is permissible, call setup is attempted. If the call cannot be completed immediately because of a busy line, line status is periodically checked until both stations are idle.
- *Automatic Recall* is an incoming Call Management feature very similar to Automatic Callback. This service enables a customer to perform an activation procedure and automatically redial the last incoming number without having to know the number of the calling party.

B.6.2 Internetwork Needs

In the future, when a Call Management subscriber in one network communicates with another network, internetwork TCAP messaging will occur as queries and responses are sent (e.g., to determine line status). For this reason, an internetwork Translation Type code value is required.

B.6.3 Involved Nodes

The SEP serving the Call Management subscriber generates a TCAP query message that requires Global Title Translation routing at one or more STPs. This query message is ultimately routed to the node serving the Call Management application. Figure B-7 is an illustration of a query and response.

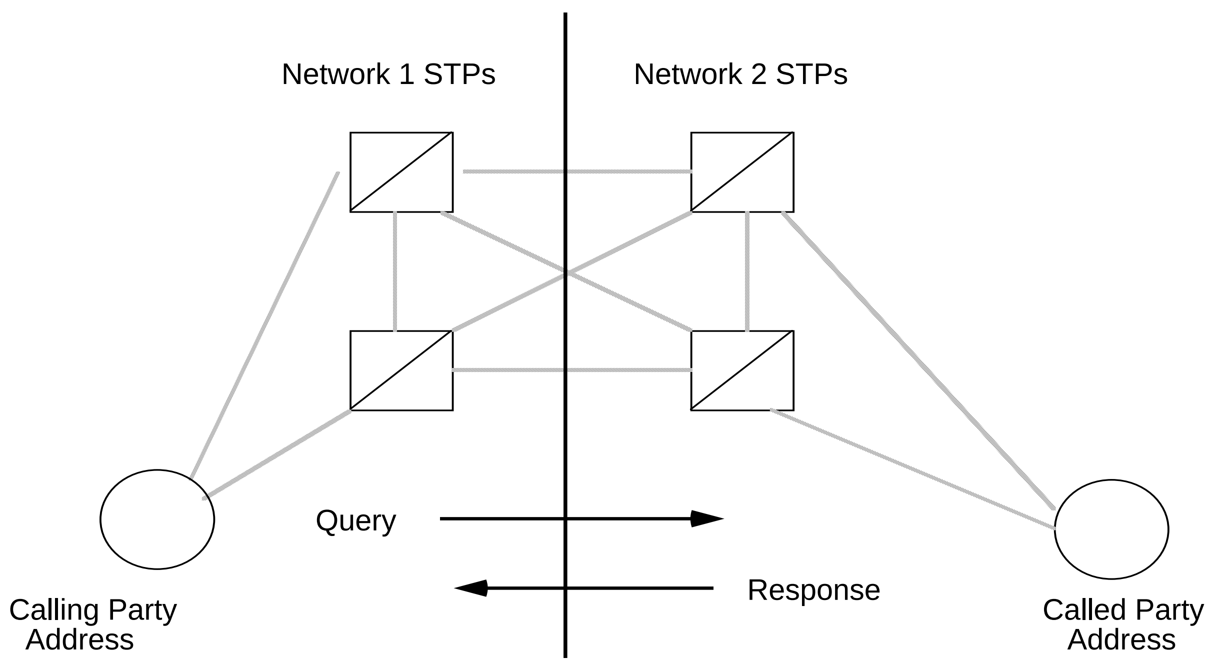


Figure B-7/ATIS-1000112.3 - Call Management Example Diagram

B.6.4 Global Title Translation Requirements

The global title address information contains the ten-digit North American Numbering Plan called party number in the format of NPA+NXX+XXXX. This address information is encoded as BCD. Global Title Indicator type of 2 will be used.

It is expected that either 3 or 6-10 digits of the Global Title Address Information will be used for GTT. The output of the final Global Title Translation will be the point code of the SEP serving the Called Party and SSN of the application.

B.6.5 Relationship to Existing Application/Translation Groups

The Global Title Address information in this application/translation group is the same as in other existing groups; however, this application requires independently allocated resources and management from existing groups (i.e., the output of the global title translation must be the Call Management application at the SEP).

B.7 TRANSLATION TYPE CODE VALUE: 00000111 (7)

Application/Translation Group: *Message Waiting*

B.7.1 Application Description

Message Waiting Services are a set of features that will use the CCS network to pass parameters from the subscriber's office to the Message Storage System (MSS) service provider's network. These services are defined in ATIS standards as T1.622, *Message Waiting Indicator Control and Notification Supplementary Services and Associated Switching and Signaling Specifications*. The parameters are sent with call setup messages from the subscriber to the MSS. The Message Waiting services are applications that also will use the TCAP layer of the protocol. The TCAP layer is used to pass parameters from the MSS to the subscriber's office to activate/deactivate an indicator on the status of the subscriber's message waiting indicator. GTTs are done at one or more STPs to identify the network node that serves the subscriber's Called Party Address (NPA-NXX).

B.7.2 Internetwork Needs

In the future, when an MSS in one network communicates with a Message Waiting subscriber in another network to modify the subscriber's Message Waiting indicator, internetwork TCAP Messaging will occur.

B.7.3 Involved Nodes

The SEP serving the MSS generates a TCAP query message that requires Global Title Translation routing at one or more STPs. This query message is ultimately routed to the node serving the Message Waiting Subscriber. Figure B-8 illustrates an example of a query.

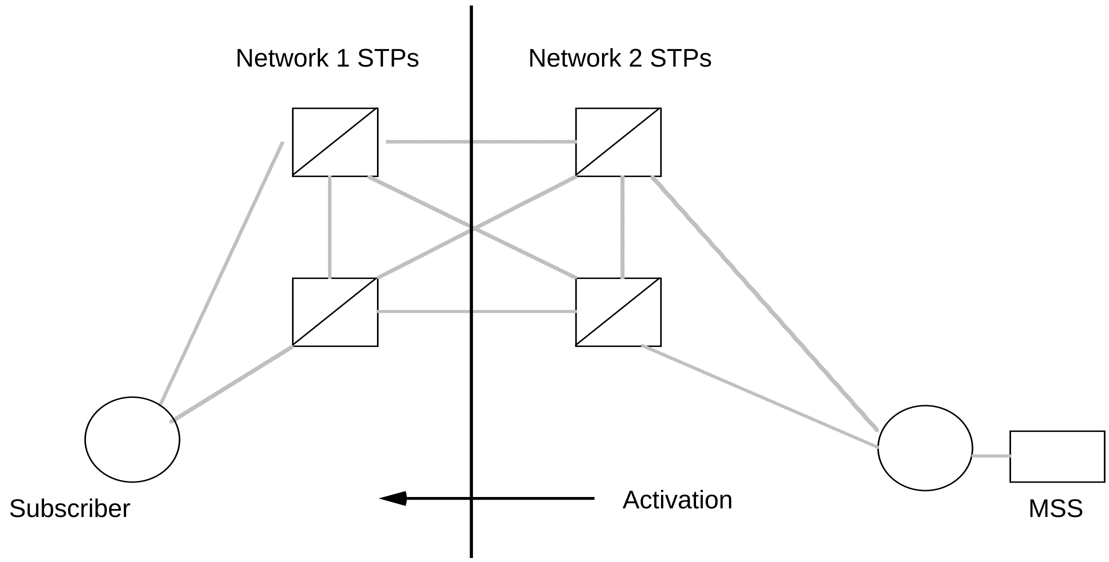


Figure B-8/ATIS-1000112.3 - Message Waiting Example Diagram

B.7.4 Global Title Translation Requirements

The global title address information contains the ten-digit North American Numbering Plan subscriber's called party address in the format of NPA+NXX+XXXX. This address information is encoded as BCD. Global Title Indicator type 2 will be used.

It is expected that either 3 or 6-10 digits of the Global Title Address Information will be used for GTT. The output of the final Global Title Translation will be the point code of the SEP serving the subscriber's called party address and SSN of the application.

B.7.5 Relationship to Existing Application/Translation Groups

The Global Title Address information in this application/translation group is the same as in other existing groups; however, this application requires independently allocated resources and management from existing groups (i.e., the output of the global title translation must be the Message Waiting application at the SEP).

B.8 TRANSLATION TYPE CODE VALUE: 00001000 (8)

Application/Translation Group: *SCP-Assisted Call Processing Application*

B.8.1 Application Description

Applications residing at an SCP affect switch call processing by exchanging TCAP messages with switches (or with other SCPs). Such an exchange is typically initiated by a switch detecting a call related event that matches provisioned criteria (e.g., a particular digit string being dialed). This event is referred to as a *trigger*. A trigger may cause a TCAP query to be sent to an associated application in an SCP. Via TCAP messages, the SCP application performs its function by -- for example -- directing the switch to route a call to a particular destination or to interact with the customer by playing voice announcements and collecting digits entered by the customer. The functionality needed to support this type of call processing includes:

- *Origination Attempt* - Allows the detection of a new call attempt by a calling party. This is equivalent to an off-hook indication from a non-ISDN line or the receipt of a SETUP message from an ISDN interface.
- *Info. Collected* - Allows the detection of the point in call processing when complete information has been received from the caller.
- *Info. Analyzed* - Allows the detection of the point in call processing when address information has been analyzed and the switch is ready to set up the call.
- *Network Busy* - Allows the detection of the case when all routes are found busy for the call.
- *Termination Attempt* - Allows the detection of a new call attempt to a called party. This occurs on the terminating end of the call.

Some services and architectures require communication between SCPs. For example, an SCP that is queried by a switch may need to query another SCP to obtain customer data. Global title routing of such inter-SCP messages also falls within this application/translation group.

The following are examples of applications that could be included in this application/translation group:

- *Outgoing Call Screening* - Allows a subscriber to control toll usage by implementing toll restrictions that are tailored to specific user needs. The subscriber sould have the ability to restrict calls per user based on NPA, NXX, time-of-day, day-of-week, and day-of year.
- *Automatic Call Distribution* - Distributes incoming calls to the subscriber's users or user groups who are assigned to handle specific calls (e.g., order entry, service, information).
- *Customer Call Routing* - Provides flexible routing control of local area incoming calls for a medium to large business.

A given customer can, based on customer and/or trigger identity, access multiple SCP-assisted call processing applications. If these applications use the same translation type, this places a special burden on the Global Title Address to distinguish multiple SCP-assisted call processing applications, which may or may not reside on different SCPs.

This application/translation group meets these special needs by logically splitting the Global Title Address into two parts:

1. A Location-Specific Part; and
2. An Application-Specific Part.

Originating and intermediate networks use only the Location-Specific Part, which identifies the destination STP (i.e., the STP performing the final GTT). The Application-Specific Part identifies the SCP and subsystem within the destination network. The destination STP performs GTT on the whole Global Title Address (both parts) to derive the destination Point Code and Subsystem Number.

Any SCP-assisted call processing applications requiring the use of this split Global Title Address may be included in this application/translation group. This application/translation group does not preclude other SCP-assisted call processing applications from using other distinctive translation types. In particular, this application/translation group should not be used in place of more specific existing application/translation groups.

B.8.2 Internetwork Needs

The network node (SCP) that contains the call processing service logic or customer information may not reside in the network of origination, therefore, internetwork messages will occur. For this reason, an internetwork translation type code value is required.

B.8.3 Involved Nodes

The transport of SCP-assisted call processing messages will normally involve an originating switch or SCP, one or more STPs, and a destination SCP. Figure B-9 shows an example of network interconnection in which a switch or SCP in one network generates a TCAP query message requiring GTT routing at one or more STPs, and being ultimately routed to the SCP in another network.

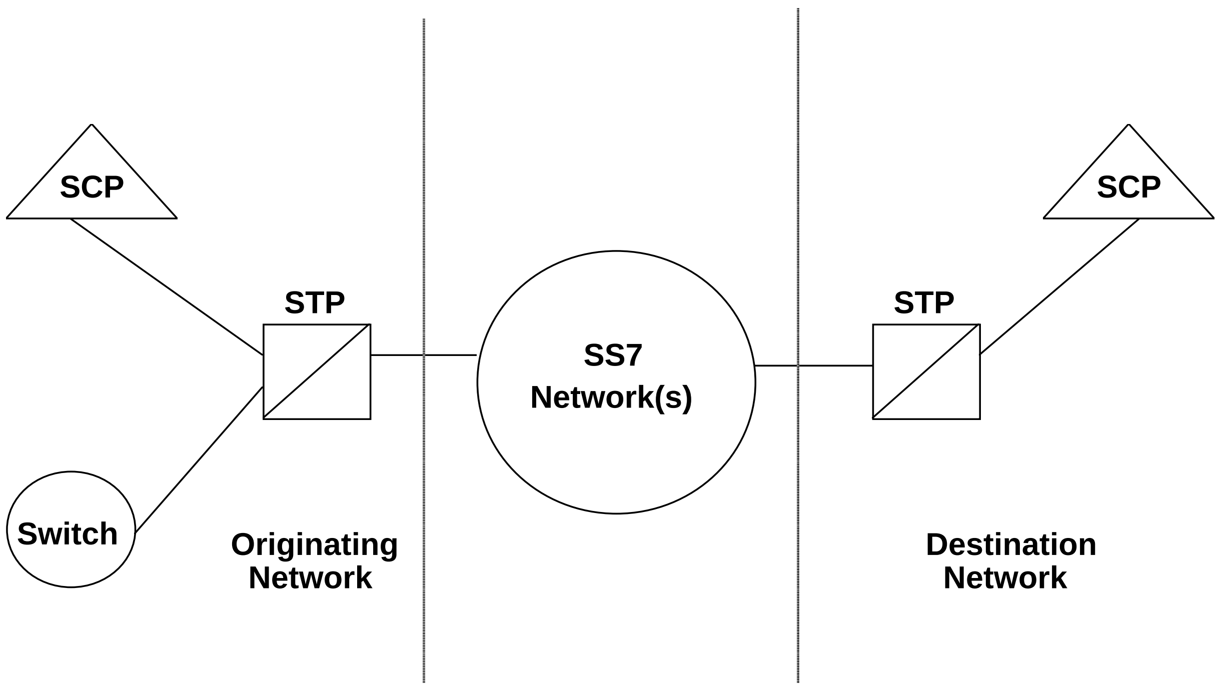
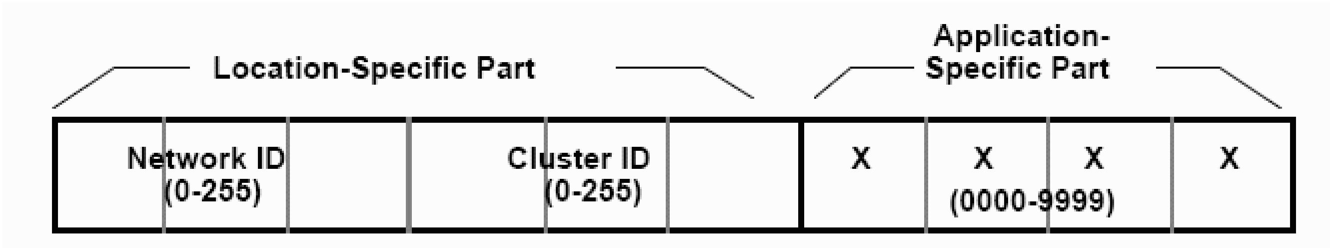


Figure B-9/ATIS-1000112.3 - SCP-Assisted Call Processing Application Example Diagram

B.8.4 Global Title Translation Requirements

The Global Title Address information contains a ten-digit number. This address information is coded according to US standards, with an encoding scheme of BCD. Global Title Indicator type 2 will be used.

The following figure illustrates the format of the 10-digit global title address:



The first 6 digits of the Global Title Address is the Location-Specific Part, and consists of the Network ID and Cluster ID of the destination STP. Note that these values are the first two bytes of a point code, but when encoded in BCD, they occupy 3 bytes. Originating and terminating networks need only the Location-Specific Part for GTT.

The last 4 digits constitute the Application-Specific Part, which identifies the destination SCP and application. The Application-Specific Part is used and administered only by the destination network. The destination STP performs GTT on the full ten-digit Global Title Address.

B.8.5 Relationship to Existing Application/Translation Groups

The translation requirements for this application/translation group differ from those described in the other application/translation groups. In addition, this application/translation group requires independently allocated resources and management from existing groups.

B.9 TRANSLATION TYPE CODE VALUE: 00001001 (9)

Application/Translation Group: *National and International Cellular/PCS Roaming*

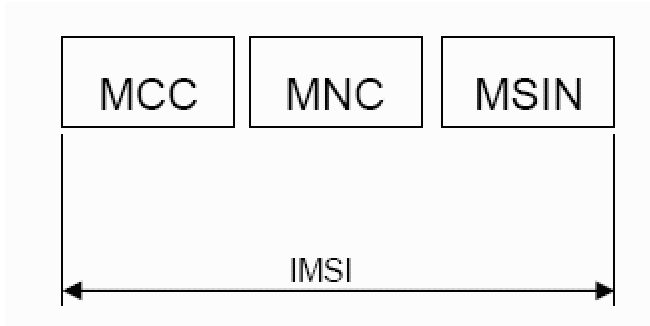
B.9.1 Application Description

One of the key requirements of wireless networks is that they should provide for both national and international roaming. Subscribers of a given North America network should be able to roam to other networks both within and outside North America and receive service. It should be possible for subscribers from networks outside of North America to come to North America and receive service from North American networks. There are two distinct applications for this translation type.

B.9.1.1 IMSI to HLR

When a subscriber roams to a network, the node that will provide service is called a Mobile Switching Center (MSC). Each such node will have a Visited Location Register (VLR) associated with it. In order for the MSC to provide service, it must communicate with the appropriate node in the subscriber's home network to inform the home network of the subscriber's location and to retrieve information about the subscriber. The node in the home network is known as the Home Location Register (HLR).

The only information available to the serving MSC, to allow it to communicate with the subscriber's HLR is the information provided by the subscriber's terminal when it makes contact with the network. This information is in the form of the International Mobile Station Identity (IMSI) and has the format below as defined in the ITU-T Recommendation E.212. (Note that for ANSI-41 networks, the terminal may provide a Temporary Station Identity (TMSI) that the MSC uses to obtain the IMSI.)



MCC = Mobile Country Code (3 digits)

MNC = Mobile Network Code (Nationally assigned, max 3 digits in USA)

MSIN = Mobile Station Identification Number

IMSI = International Mobile Station Identity (max. 15 digits)

When the MSC receives the IMSI, it uses it to address the subscriber's HLR. This is done by sending a connectionless SCCP message to the HLR using the IMSI as the Global Title (GT) address. Intervening STP's perform GTT to establish the DPC and SSN of the HLR.

Note that the IMSI is an E.212 number. It is not a dialable number and does not conform to the E.164 or to the North American Numbering Plan. It is a number used to identify the subscriber within and between wireless networks. It is separate from the number that is dialed when calling the subscriber.

B.9.1.2 E.212 to Any Network Node (for ANSI-41 Networks)

A wireless network node may need to communicate with other wireless network nodes, including the originating or gateway MSC for call redirection. This translation type may be used to communicate with any network element that is identified by an E.212 formatted address on the same, or a different, national SS7 network.

Any wireless network node may be identified by an E.212 number.

B.9.2 Internetwork Needs

The internetwork needs of this application group are to support roaming between different networks, specifically for the applications of Authentication, Registration and Location Update.

B.9.3 Involved Nodes

Several types of node will be involved in the generation, transport and reception of messages routed with an E.212 GT address, including:

- HLR, MSC, and SS7 STP's in the home network.
- MSC/VLR and SS7 STP's of the visited network.

♦ SS7 STP's of intermediate transport networks.

The following scenario provides an example of such information exchange, where the terminating node (the HLR) is addressed using an E.212 IMSI of the subscriber.

In this scenario, a subscriber from one network has roamed to another network, known as the visited network. When the subscriber registers in the visited network (by powering on the terminal), the MSC/VLR of the visited network obtains the IMSI and uses it as an addressing mechanism to communicate with the HLR in the subscriber's home network.

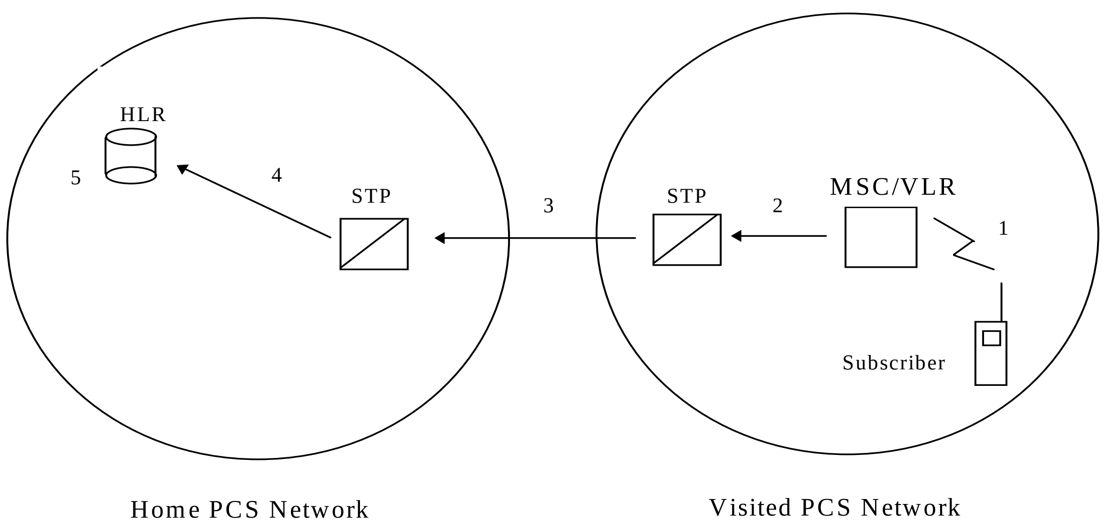


Figure B-10/ATIS-1000112.3 - Involved Nodes for PCS Roaming

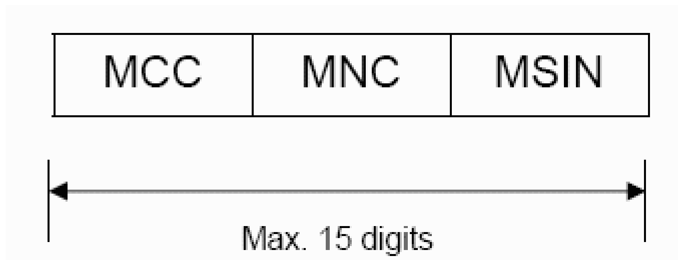
In the diagram, the subscriber has roamed to the visited PCS network and he turns on his terminal.

1. Subscriber switches on his terminal and the subscriber's IMSI (E.212) or TMSI (when appropriate) is transmitted to the MSC/VLR.
2. The MSC/VLR generates a connectionless SCCP message and populates the GT address of the called party with the IMSI digits.
3. Interconnecting SS7 signaling.
4. STP in the home network performs GTT and establishes the DPC and SSN of the HLR.
5. The HLR updates its records and is now in a position to send the subscriber data to the MSC/VLR.

The above example shows a case where the subscriber has roamed to another network within North America. It is also possible to roam internationally. Since E.212 is an internationally accepted standard, it can also be used for international roaming.

B.9.4 GlobalTitle Translation Requirements

Global Title Address Information contains an E.212 IMSI number as follows:



MCC – Mobile Country Code (3 digits)

MNC – Mobile Network Code (Nationally assigned, maximum 3 digits).

MSIN fulfills the remaining digits the GT address.

The Global Title Indicator is 0010.

The digits of the GT Address are coded in BCD.

For the IMSI to HLR translation:

- When the MCC indicates a North American network, IMSI contains 15 digits. It is expected the first 6 digits will be used to perform the GTT to route to the destination network. It is expected 6 to 10 digits will be used to perform the final GTT.
- When the MCC indicates a Non-North American network, IMSI contains 6 to 15 digits. It is expected the first 6 digits will be used to perform the GTT to route outside North America.

For E.212 to any ANSI-41 Network Node translation:

- When the MCC indicates a North American network, the GT address contains 15 digits. It is expected the first 6 digits will be used to perform the GTT to route to the destination network. It is expected that all E.212 digits (up to 15 digits) will be used to perform the final GTT.
- When the MCC indicates a Non-North American network, the GT address contains 6 to 15 digits. It is expected the first 3 to 6 digits will be used to perform the GTT to route outside North America.

B.9.5 Relation to Existing Applications/Translation Groups

There are some similarities between this application and that defined by the Translation Type (TT) value 3. However, TT value 3 is defined for Cellular Nationwide Roaming and, as such, does not address the needs of international roaming. Furthermore, TT value 3 relates to a GT address that complies with the North American Numbering Plan. E.212 does address the needs of international roaming and does not comply with the North American Numbering Plan.

There is no existing TT value that meets the need of this application.

Assignment of a new TT value for this application will not affect other application/translation groups.

B.10 TRANSLATION TYPE CODE VALUE: 00001010 (10)

Application/Translation Group: *Network Entity Addressing*

B.10.1 Application Description

PCS 1900 network entity addressing uses E.164 numbers that are not considered portable.

Prior to the deployment of Number Portability (NP), SCCP routing to either a Network Entity (NE) or a Mobile Station International ISDN Number (MSISDN) uses Translation Type 10. After the deployment of of NP, addressing to the MSISDN is accomplished through the use of Translation Type 14, Translation Type 10 will only be used for Network Entity addressing.

The recommendation on the assignment of these two Translation Type values is as follows:

- ♦ Messages that are SCCP routed using NE E.164 addresses should be assigned Translation Type 10.
- ♦ Messages that are SCCP routed using MSISDN E.164 addresses should be assigned Translation Type 14.

B.10.2 Internetwork Needs

This application group supports routing of SS7 MAP messages in which a Network Entity E.164 address is used as global title in the SCCP Called Party Address.

B.10.3 Involved Nodes

B.10.3.1 Type of Nodes

The most common types of nodes involved in the generation, transport and reception of messages routed to a Network Entity E.164 address are as follows:

- ♦ Originating Node: MSC, HLR, or VLR
- ♦ Transport Node: STP or GMSC
- ♦ Destination Node: SC, HLR, VLR, or MSC.

The originating node will assign Translation Type 10 when the GTA in the SCCP Called Party Address contains the E.164 address of a NE.

B.10.3.2 Example of Routing Mobile Originated SMS-PP

PCS 1900 networks use entity addressing for multiple network functions (e.g., authentication, supplementary service programming, MAP provide roaming number, mobile originated SMS-PP, delivery of MAP forward short messages, etc.). All of these messages use a non-portable E.164 entity address for inter-network routing.

Using Mobile Originated SMS-PP as an example, SS7 MAP messages are routed from a short message entity to the called subscriber's Short Message Service Center (SC).

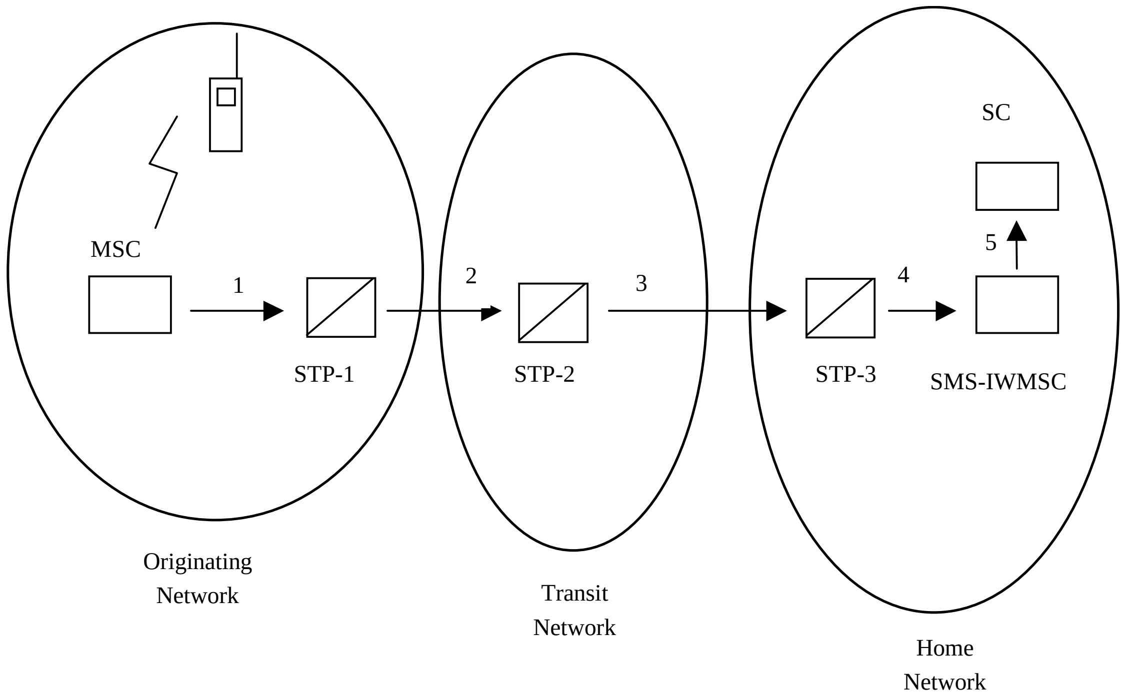
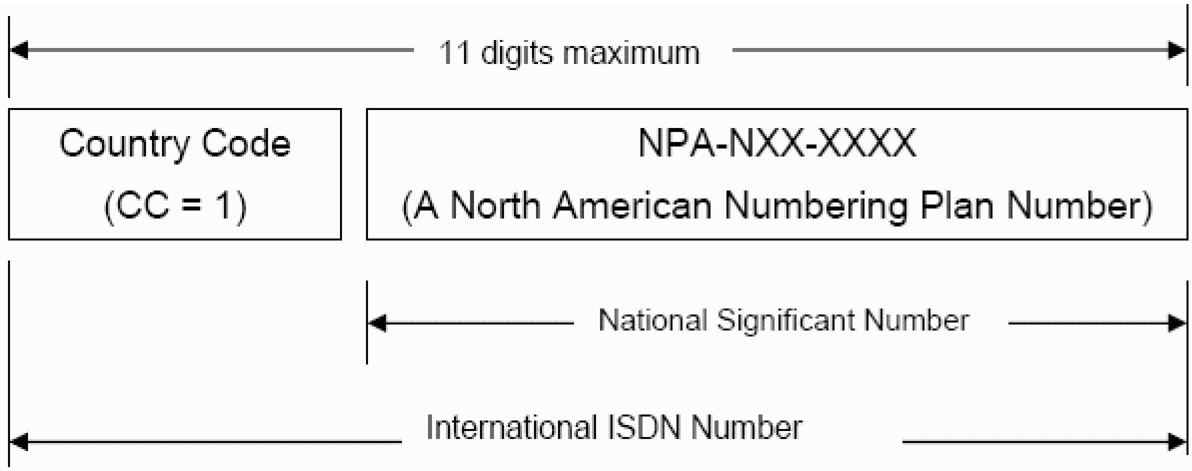


Figure B-11/ATIS-1000112.3 – Delivering PCS 1900 Mobile Originated SMS-PP to a SC

1. The MSC receives the SM from the mobile, which is then forwarded to the STP-1 in the same network, as a MAP message (MAP_FORWARD_SM). This message contains the E.164 address of the SC in the global title of the SCCP called party address. Because this is a network entity address, the SCCP translation type is set to the E.164 translation type 10.
2. STP-1 translates the country code "1" and NPA-NXX portion of the SCCP E.164 address. The translation results in the signaling point code of STP-2 to which the message is then routed.
3. STP-2 translates the country code "1" and the NPA-NXX portion of the SCCP E.164 address. The translation results in the signaling point code of STP-3 to which the message is then MTP routed.
4. STP-3 forwards the SM (MAP_FORWARD_SM) to the SMS-IWMSC in the same network.
5. The SMS-IWMSC forwards the message (MAP_FORWARD_SM) to the SC.

B.10.4 Global Title Translation Requirements

The format of the network entity (NE) address in the Global Title Address (GTA) is based on the E.164 numbering plan. For Integrated Numbering Plan with CC = 1, the format is as follows:



E.164 Number Format for CC = 1

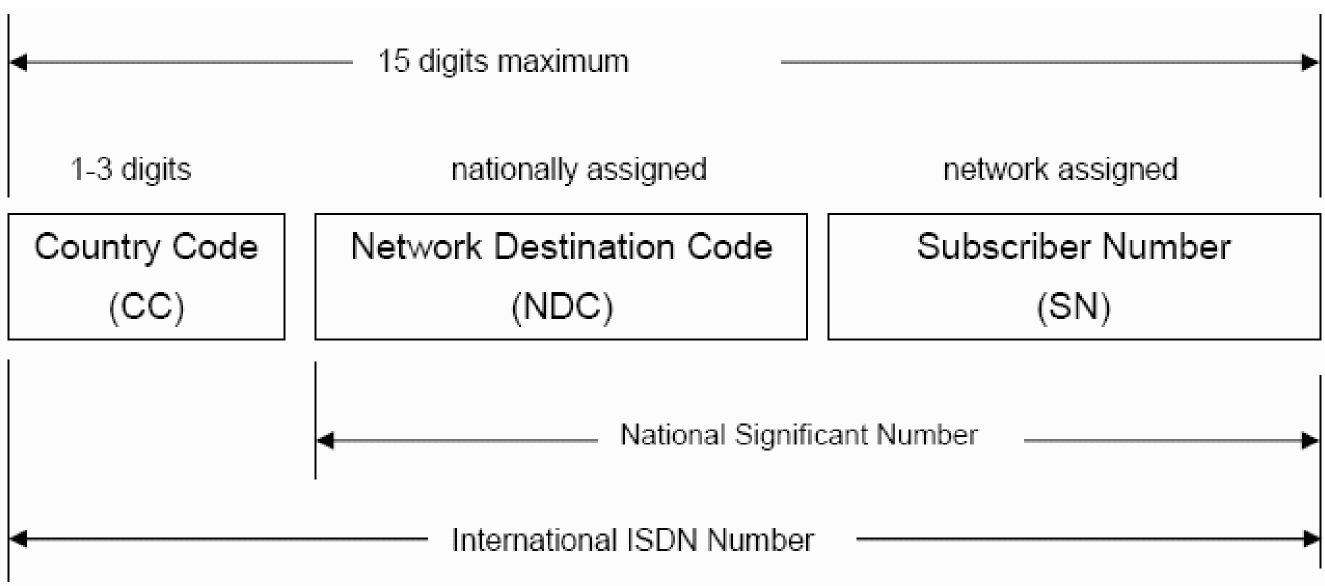
When CC = 1, the maximum length of the NE address in the E.164 GTA is 11 digits.

The Global Title indicator is 0010.

The digits of the GTA are Binary Coded Decimal in 1/2 octet per digit.

When the CC = 1, the NE address in the E.164 GTA contains 11 digits. Global title translation on the first seven digits is required to route to the destination network. GTT on all eleven digits may be required for delivery to the final destination. The output of the final GTT is the DPC and SSN of the destination to which the message is being routed.

When CC is not equal to 1, the format of the NE address in the E.164 GTA is as follows:



E.164 Number Format For Other Than CC = 1

The maximum length of the GTA information for the other than CC = 1 NE address is the maximum allowed by the E.164 numbering plan (up to 15 digits).

The country code (CC) is 1-3 digits.

The National Destination Code (NDC) length depends on the country in question.

The SN is the subscriber number.

The Global Title Indicator is 0010.

The digits of the GTA are coded in Binary Coded Decimal of 1/2 octet per digit.

When the CC is not equal to 1, the E.164 GTA information contains the maximum allowed by the numbering plan. Global Title Translation on 1-3 digits is required to route to the destination country. The output of the final GTT is the DPC and SSN of the destination to which the message is being routed.

B.10.5 Relationship to Existing Application/Translation Groups

Before Number Portability, Translation Type 10 was sufficient for SCCP routing to both PCS 1900 MSISDN addresses and PCS 1900 NE addresses. With the advent of NP, Translation Type 14 is used for MSISDN addresses and Translation Type 10 is used for NE addresses.

Assignment of a new TT value for this application will not affect other application/translation groups.

B.11 TRANSLATION TYPE CODE VALUE: 00001011 (11)

Application/Translation Group: *Internetwork NP Query/Response (NP Q/R)*

B.11.1 Application Description

NP (Number Portability) refers to the network capability that allows end users to retain their telephone number when they change their service provider, their location, or their service. One of the key functions of NP requires the initiating switch to send a query to the NP database to determine the network routing address of the ported end user's serving switch. The NP database will translate the portable address received in the NP query to a network routing number, and send it back to the NP initiating switch in the response message. Essentially, the NP query messages, using the services of SCCP, will require GTT at one or more STPs to identify the NP database.

B.11.2 Internetwork Needs

If the NP initiating switch and the NP database are in different networks, the internetwork TCAP query and response will be exchanged across the network boundary to determine the network routing address. For this reason, an internetwork translation type code value is required.

B.11.3 Involved Nodes

The NP initiating switch that serves as the query node, generates a TCAP query message that requires GTT routing at one or more STPs. This query message is ultimately routed to the node acting as the NP database, as illustrated in Figure B-12/ATIS-1000112.3. Depending on the trigger mechanisms that are used in the initiating switch, the given NP database may need to support multiple protocols (AIN, IN, etc.). Furthermore, the Translation Type assigned to this application group may be used to route a query message to multiple SCP database configuration, such as load sharing, primary/backup, or primary/multiple backups, if needed in the near future.

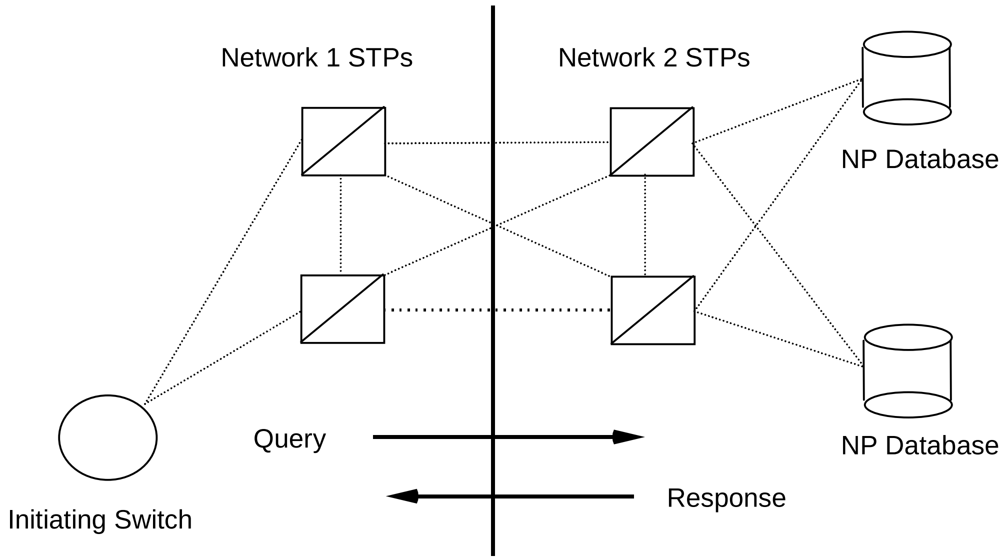


Figure B-12/ATIS-1000112.3 – Internetwork NP Query/Response

B.11.4 Global Title Translation Requirements

The GTA information in the Called Party Address (CdPA) of an SCCP message contains the ten-digit North American Numbering Plan (NANP) portable address in the format of NPA-NXX-XXXX. This address is encoded as BCD, and Global Title Indicator type of two (2) will be used. It is expected that the new Translation Type will be used to transport the internetwork query messages to the NP database.

In addition, depending on the implementation, 0-10 (0, 3, 6, or 10) digits of the global title address information can be used for GTT. The output of the final GTT will be the Point Code and SSN of the destination NP database.

B.11.5 Relationship to Existing Application/Translation Groups

The global title address information in this application / translation group is the same as in a few other existing groups; however, this application requires independently allocated resources and management (i.e., the output of the GTT must be the NP database).

The assignment of a new Translation Type code value for this application will not affect other application / translation groups.

B.12 TRANSLATION TYPE CODE VALUE: 00001100 (12)

Application/Translation Group: Wireless MIN-Based *Short Message Service*

B.12.1 Application Description

Wireless MIN-Based Short Message Service allows wireless subscribers to request and receive subscribed-to short message services (SMS) while roaming in any system, just as they would in their home system. Short messages may be originated by (or terminated at) mobile station based Short Message Entities (SME). An SME is an entity that is capable of composing and disposing short messages. A key procedure to the successful offering of mobile originated short message service is ability for a mobile station based SME to deposit a short message at its Message Center (MC) in its home system, even while the mobile station is roaming. The MC is a store and forward network entity, and every MS-based SME is associated with one and only one MC.

The mobile station passes information such as its Mobile Identification Number (MIN), and the short text message over the radio air interface to the serving Mobile Switching Center (MSC) when the user initiates a short message delivery service request. The serving MSC could be in either the MS's home system or a visited system. The wireless industry uses the MIN as the global title to route a ShortMessageDeliveryPointToPoint (SMDPP) TCAP message with an INVOKEComponent, a TIA IS-41 Mobile Application Part (MAP) message, from the MSC in a visited system to the subscriber's Message Center in the home system, over inter-connecting SS7 networks. Using the GTT capability of the SS7 networks frees the wireless system from performing GTT-like translation (e.g., mapping the MIN to an SS7 point code and SSN). The short text message is then passed on to the MC, where it is stored, and then forwarded to the terminating SME (which could be mobile station based or otherwise).

B.12.2 Internetwork Needs

The transport of a SMDPP TCAP message with an INVOKE Component (as a result of a short message delivery service request originating from a roaming mobile station) will typically involves the serving MSC in the visited system, the Message Center in the home system, and interconnecting SS7 networks.

B.12.3 Involved Nodes

Figure B-13/ATIS-1000112.3 shows the nodes and systems involved in the message transport between the serving MSC in the visited system and the Message Center in the home system. The serving MSC in the visited system sends out the SMDPP TCAP message with an INVOKE Component to the interconnecting SS7 network when it receives the short message delivery service request originating from the roaming mobile station. The MIN is used as the global title address information in the SCCP Called Party Address field.

The interconnecting SS7 network then performs the GTT and translates the GT (the MIN) into an SS7 point code and SSN for the MC. Several STPs in the interconnecting SS7 network may be involved in the message routing. One of them performs the final GTT, which translates the global title into an SS7 point code and SSN.

When the MC receives the SMDPP TCAP message with an INVOKE Component, it responds with a TCAP message ~~with~~ containing a~~n~~ Return Result Component with the appropriate contents (such as positive or negative acknowledgements). The TCAP message with the RETURN RESULTComponent is routed back to the serving MSC in the visited system through the interconnecting SS7 network by MTP routing. In the case of a positive acknowledgement, the MC will proceeds to store the short text message, and attempts to forward the short text message to the recipient SME when that SME becomes available (not shown in Figure B-13/ATIS-1000112.3).

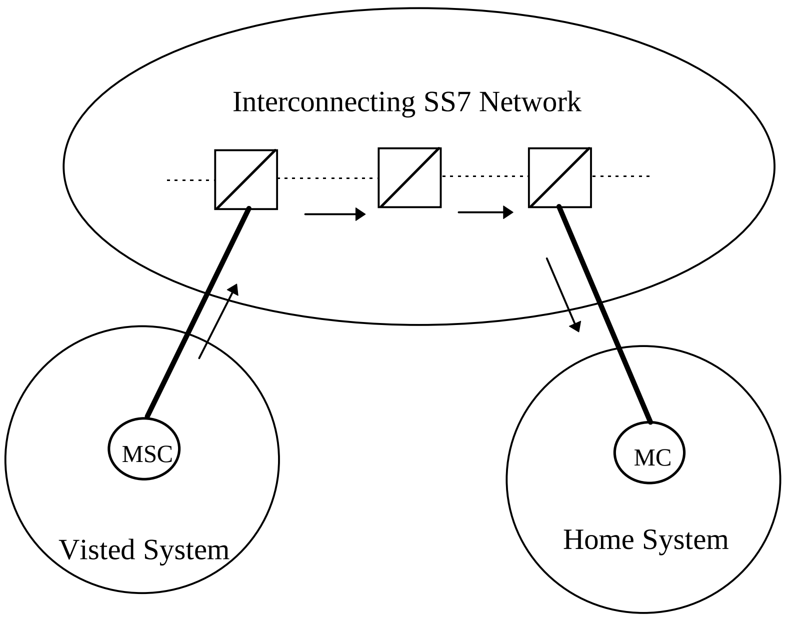


Figure B-13/ATIS-1000112.3 - Involved Nodes When Routing An SMDPP from an MSC to the MC

B.12.4 Global Title Translation Requirements

The global title address information contains the MIN, which is a ten-digit North American Number Plan number with the format NPA+NXX+XXXX. The numbering plan is ISDN Numbering Plan (E.164) and only the national number portion is used as the global title address. The encoding scheme is BCD. Each address signal is coded as described in clause 3.4.2.3.1 of ATIS-1000112.3. Global Title Indicator type 2 is used.

It is expected that only 6 to 9 out of the 10 digits of the global title address information should be used to perform the GTT. The output of the final GTT is the point code and SSN of the MC.

B.12.5 Relationship to Exiting Application/Translation Groups

The IS-41 MAP uses the ANSI TCAP Component and Translation Sub-layer facilities to communicate. The IS-41 MAP uses private operation codes, private error codes, and context-specific parameter identifiers. Therefore, its usage of the TCAP does not impact other application/translation groups. The application procedures of the Wireless MIN-Based Short Message Service are described in the TIA IS-41 document.

Existing application/translation groups remain unaffected with respect to the new resource/management needs for this application/translation group.

B.13 TRANSLATION TYPE CODE VALUE: 00001101 (13)

Application/Translation Group: Wireless IMSI-Based Short Message Service

B.13.1 Application Description

Wireless IMSI-Based Short Message Service allows wireless subscribers to request and receive subscribed-to SMS while roaming in any system, just as they would in their home system. Short messages may be originated by (or terminated at) mobile station based SMEs. An SME is an entity that is capable of composing and disposing short messages. A key procedure to the successful offering of mobile originated short message service is ability for a mobile station based SME to deposit a short message at its MC in its home system, even while the mobile station is roaming. The MC is a store and forward network entity, and every MS-based SME is associated with one and only one MC.

The mobile station passes information such as its International Mobile Station Identity (IMSI), and the short text message over the radio air interface to the serving MSC when the user initiates a short message delivery service request. The serving MSC could be in either the MS's home system or a visited system. The wireless industry uses the IMSI as the global title to route a SMDPP TCAP message with an INVOKEComponent, a TIA IS-41 MAP message, from the MSC in a visited system to the subscriber's Message Center in the home system, over inter-connecting SS7 networks. Using the GTT capability of the SS7 networks frees the wireless system from performing GTT-like translation (e.g., mapping the IMSI to an SS7 point code and SSN). The short text message is then passed on to the MC, where it is stored, and then forwarded to the terminating SME (which could be mobile station based or otherwise).

B.13.2 Internetwork Needs

The transport of a SMDPP TCAP message with an INVOKE Component (as a result of a short message delivery service request originating from a roaming mobile station) typically involves the serving MSC in the visited system, the Message Center in the home system, and interconnecting SS7 networks.

B.13.3 Involved Nodes

Figure B-14/ATIS-1000112.3 shows the nodes and systems involved in the message transport between the serving MSC in the visited system and the Message Center in the home system. The serving MSC in the visited system sends out the SMDPP TCAP message with an INVOKE Component to the interconnecting SS7 network when it receives the short message delivery service request originating from the roaming mobile station. The IMSI is used as the global title address information in the SCCP Called Party Address field.

The interconnecting SS7 network then performs the GTT and translates the GT (the IMSI) into an SS7 point code and SSN for the MC. Several STPs in the interconnecting SS7 network may be involved in the message routing. One of them performs the final GTT, which translates the global title into an SS7 point code and SSN.

When the MC receives the SMDPP TCAP message with an INVOKE Component, it responds with a TCAP message with a RETURN RESULT Component with the appropriate contents (such as positive or negative acknowledgements). The TCAP message with the RETURN RESULT Component is routed back to the serving MSC in the visited system through the interconnecting SS7 network by MTP routing. In the case of a positive acknowledgement, the MC proceeds to store the short text message, and attempts to forward the short text message to the recepient SME when that SME becomes available (not shown in Figure B-14/ATIS-1000112.3).

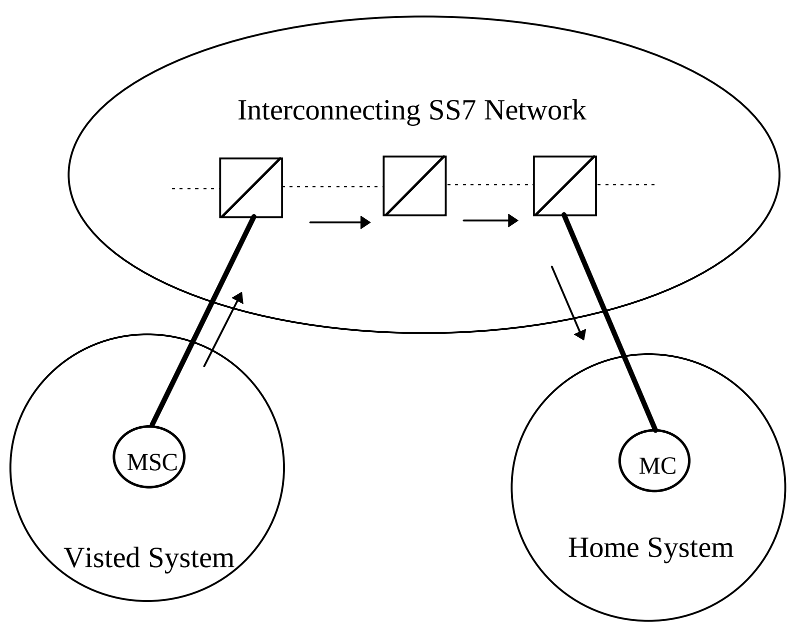


Figure B-14/ATIS-1000112.3 - Involved Nodes When Routing an SMDPP from an MSC to the MC

B.13.4 Global Title Translation Requirements

The global title address information contains the IMSI, which is 15 digits long. The numbering plan follows E.212. The encoding scheme is BCD. Global Title Indicator type 2 is used.

When the MCC indicates a North American network, IMSI contains 15 digits. It is expected the first 6 digits should be used to perform the GTT to route to the destination network. It is expected 6 to 10 digits may be used to perform the final GTT.

When the MCC indicates a Non-North American network, IMSI contains 6 to 15 digits. It is expected the first 6 digits should be used to perform the GTT to route outside North America.

The output of the final GTT is the point code and SSN of the MC.

B.13.5 Relationship to Existing Application/Translation Groups

The IS-41 MAP uses the ANSI TCAP Component and Translation Sub-layer facilities to communicate. The IS-41 MAP uses private operation codes, private error codes, and context-specific parameter identifiers. Therefore, its usage of the TCAP does not impact other application/translation groups. The application procedures of the Wireless IMSI-Based Short Message Service are described in the TIA IS-41 document.

Existing application/translation groups remain unaffected with respect to the new resource/management needs for this application/translation group.

B.14 TRANSLATION TYPE CODE VALUE: 00001110 (14)

Application/Translation Group: *Mobile Subscriber Addressing*

B.14.1 Application Description

When a call or a service such as mobile terminated point-to-point short message is identified as being directed to a PCS1900 Mobile Subscriber, the originating or gateway node must query the HLR of the MS for routing information. To reach the home HLR, the PCS1900 MAP query message must be routed using the terminating MS's MSISDN as the global title in the SCCP called party address. When the HLR receives the routing query it responds with the routing information towards the MSC/VLR which is currently serving the MS.

Prior to the deployment of NP, a PCS1900 network operator can assign a number of network owned NPA-NXX codes to a particular HLR. Using the existing translation type 10, the network operator would arrange for SCCP routing tables -- in those STPs supporting this translation type -- to route SCCP messages addressed to numbers within these NPA-NXX codes to (or towards) the associated HLR. By restricting the MSISDNs served by an HLR to lie within this HLR's set of assigned NPA-NXX codes, a network operator can assure that SCCP messages addressed to these MSISDNs will be correctly routed to the HLR using SCCP GTT of only the first seven digits of the MSISDN -- comprising the E.164 country code "1" plus the 6-digit NPA-NXX portion of the MSISDN.

Following the deployment of NP, it will be possible for a PCS1900 MSISDN to belong to an NPA-NXX group that is not assigned to its home network. It will also be possible for a number within an NPA-NXX assigned to a PCS1900 network to belong to a non-PCS1900 subscriber. To ensure correct routing to the HLR in the former case and detection of the non-PCS1900 number in the latter case, it will be necessary for SCCP GTT to translate all eleven digits (i.e., the country code "1" plus NPA-NXX-XXXX digits) of any MSISDN that lies within a portable NPA-NXX range.

Following the deployment of NP, there will exist two distinct types of PCS1900 E.164 global title address: network entity addresses for which seven digit SCCP GTT will suffice and MSISDN addresses for which eleven digit SCCP GTT will be needed if the MSISDN lies in a portable NPA-NXX range. In order to reduce both the impacts of deploying NP and the possibility of SCCP GTT congestion, it is desired to continue routing PCS1900 messages addressed to network entities using the existing translation type 10 and use the SCCP translation type 14 for all messages addressed to an MSISDN.

The recommendation on the assignment of these two Translation Type values is as follows:

- Messages that are SCCP routed using Network Entity addresses should be assigned Translation Type 10; and
- Messages that are SCCP routed using MSISDN addresses should be assigned Translation Type 14.

B.14.2 Internetwork Needs

This application group supports routing of SS7 MAP messages in which an MSISDN is used as the Global Title Address (GTA) in the SCCP called party address.

B.14.3 Involved Nodes

B.14.3.1 Types of Nodes

The following types of node will be involved in the generation, transport and reception of messages routed to a PCS1900 MSISDN:

- Originating Node: MSC, SMS-GMSC, GMSC or International STP
- Transport Node: STP or NP GTT function
- Destination Node: HLR

The originating MSC or International STP will assign the translation type 14 when the global title in an SCCP called party address contains a PCS1900 MSISDN. Both nodes should then perform routing based on SCCP GTT of the first seven digits (country code "1" plus NPA-NXX) of the MSISDN. In the case of an international STP (ISTP), the origination can be considered to occur when an ITU SS7 message received from a source outside North America is reformatted into an ANSI SS7 message intended for a PCS1900 destination within North America. The ISTP can determine that a North American E.164 destination is PCS1900 either through suitable international routing agreements or by translation of the number using an NP-GTT type of function (described below) for numbers in a portable NPA-NXX range. Having determined that a North American E.164 destination address is PCS1900, an ISTP would reformat the SCCP called party address according to ANSI rules. If the ISTP is equipped with an eleven digit SCCP GTT capability that can recognize PCS1900 network entity addresses, it can continue to use the translation type 10 to route SCCP messages addressed to such entities to or towards their destination. In all other cases, the ISTP would need to include the translation type defined here for a PCS1900 MSISDN for all messages addressed to a PCS1900 E.164 address. In this case, ITU SS7 messages addressed to both PCS1900 network entity addresses and PCS1900 MSISDNs will both use the MSISDN translation type (because the ISTP would not distinguish between these two types of address). Although eleven digit SCCP GTT will then be employed in an NP GTT function for unported network entity addresses in any portable NPA-NXX range, this will still result in correct routing and should not significantly congest the NP GTT function due to the very small proportion of international PCS1900 messages compared to national messages.

Transport by STPs should employ SCCP GTT of the first seven digits (country code "1" plus NPA-NXX portion) of the MSISDN in the SCCP called party address. The STP translation result will give the signaling point code of the destination HLR, another STP or an NP GTT function. Routing to an NP GTT function will occur for an MSISDN that lies in a portable NPA-NXX range if the STP has an arrangement with any NP GTT serving this portable NPA-NXX. Transport by the NP GTT function will occur when it is necessary to perform eleven-digit SCCP GTT on a PCS1900 MSISDN lying within a portable NPA-NXX range. The requirements for the NP GTT function are as defined in T1.TRQ.3-1999, *Number Portability Database and Global Title Translation*[19].

The destination node for messages addressed to a PCS1900 MSISDN is always a PCS1900 HLR.

B.14.3.2 Example of Call delivery to a MSISDN

A mobile terminating call is illustrated in the figure below for the case where the call arrives from the PSTN. In this example, it is assumed that NP database query has been done where results include the home PLMN LRN, and that the terminating MSISDN is served by the home PLMN.

[19] This document is available from the Alliance for Telecommunications Industry Solutions, 1200 G Street N.W., Suite 500, Washington, DC 20005. <http://www.atis.org>

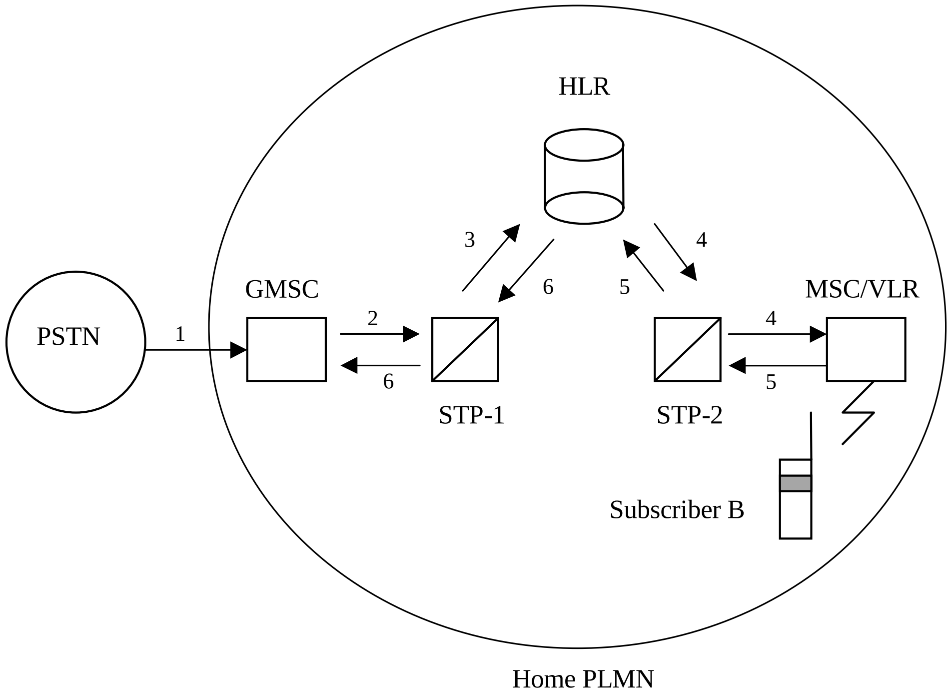


Figure B-15/ATIS-1000112.3 – Involved Nodes for PCS1900 Call Delivery

1. Call arrives at the Home PLMN of subscriber B.
2. The GMSC sends a query with TT 14 for routing information using the E.164 MSISDN as the Global Title Address information.
3. STP-1 translates the appropriate number of digits (seven or eleven) of the SCCP MSISDN address. Because the MSISDN is served by this PLNM, the translation result is the DPC and the SSN of the HLR.
4. The HLR queries the serving MSC/VLR for the roaming number.
5. The MSC/VLR responds with the MSRN.
6. The HLR sends routing information in the response back to the GMSC via STP-1.

Call setup towards subscriber B can now be carried out by the GMSC.

B.14.3.3 Example of SMS-PP Transfer to a Portable MSISDN

Routing to the HLR serving a PCS1900 subscriber to support terminating SMS-PP transfer to this subscriber is illustrated in the figure below for the case of an MSISDN in a portable number range. In this example, it is assumed that the terminating MS is served by the home PLMN and that the NP GTT function is provided in a transit network.

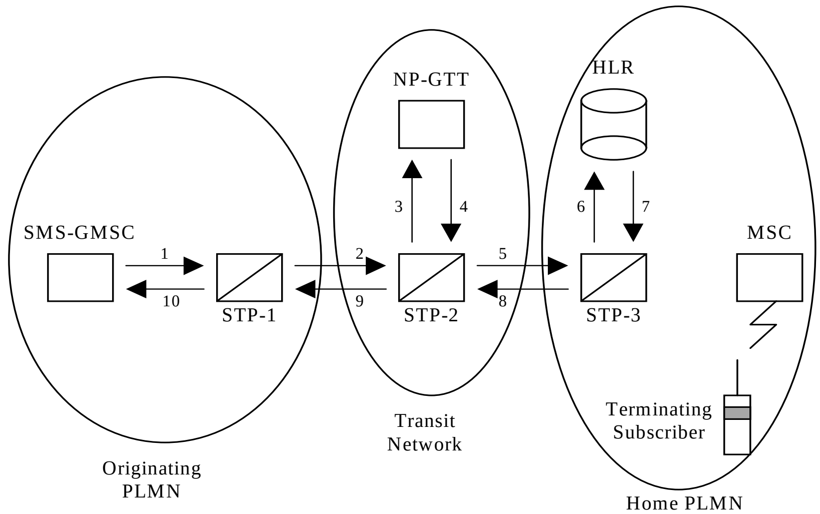


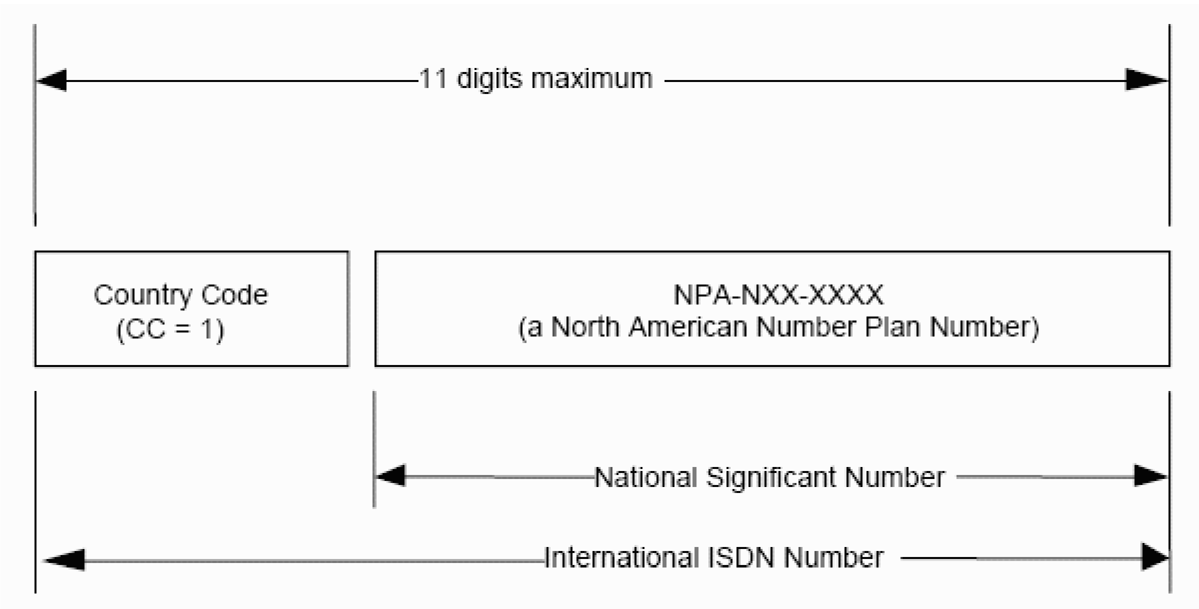
Figure B-16/ATIS-1000112.3 - Involved Nodes for PCS1900 Terminating SMS-PP Transfer

1. The SMS Gateway MSC (SMS-GMSC) responsible for delivering an SMS message to some terminating PCS1900 subscriber sends a MAP interrogation message towards the home HLR of this subscriber. This message contains the MSISDN of the subscriber in the global title of the SCCP called party address. The translation type for this address is TT 14. The message is MTP routed initially to STP-1 in the same network.
2. STP-1 translates the country code “1” and NPA-NXX portion of the SCCP MSISDN address. The translation result is the signaling point code of STP-2 to which the message is then MTP routed.
3. STP-2 translates the country code “1” and NPA-NXX portion of the SCCP MSISDN address. Because the NPA-NXX is portable, the translation result is the signaling point code of a GTT NP function. If the NPA-NXX was not portable, it would be unnecessary to route to an NP GTT function, and the translation result could be the signaling point code of STP-3; in this case, routing steps 3 and 4 to the NP GTT would be omitted.
4. The NP-GTT function translates the country code “1” and entire NPA-NXX-XXXX digits of the SCCP MSISDN address. The translation result is the signaling point code of the terminating subscriber’s HLR. The message is MTP routed towards this signaling point code via STP-2.
5. STP-2 MTP routes the message to STP-3.
6. STP-3 MTP routes the message to the HLR.
7. The HLR retrieves the E.164 address of the MSC currently serving the terminating subscriber and returns this to the SMS-GMSC. To correctly route back to the SMS-GMSC, the latter’s E.164 address (passed to the HLR by the interrogation message) is used as the global title in the SCCP called party address. Because this is a network entity address, the SCCP translation type is translation type 10. The message is routed first to STP-3 in the same network.
8. STP-3 translates the SMS-GMSC E.164 address and routes the message to STP-2.
9. STP-2 translates the SMS-GMSC E.164 address and routes the message to STP-1.

10. STP-1 translates the SMS-GMSC E.164 address and routes the message to the SMS-GMSC. The SMS-GMSC can now complete the terminating SMS-PP transfer by sending the SMS message to the MSC address returned by the HLR.

B.14.4 Global Title Translation Requirements

The format of the MSISDN in the GTA is based on the E.164 numbering plan. For Integrated Numbering Plan with CC = 1, the format is shown below.



E.164 Number Format for CC = 1

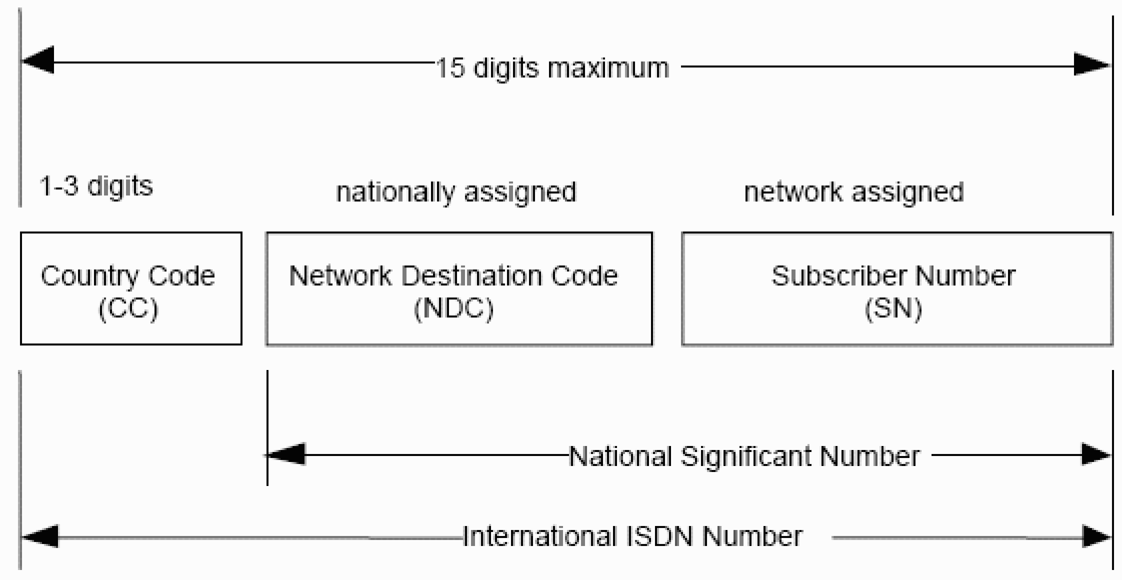
When CC = 1, the maximum length of the NE address in the E.164 GTA is 11 digits.

The Global Title indicator is 0010.

The digits of the GTA are Binary Coded Decimal in 1/2 octet per digit.

When the CC = 1, the MSISDN in the E.164 GTA contains 11 digits. Global title translation on the first seven digits is required to route to the boundaries (defined by GTT databases) of an area of portability. Within the area of portability, an eleven-digit GTT is required for delivery to the final destination network. The output of the final GTT is the DPC and SSN of the destination to which the message is being routed.

When CC is not equal to 1, the format of the NE address in the E.164 GTA is as shown below.



E.164 Number Format For Other Than CC = 1

The maximum length of the GTA information for other than CC = 1 NE addresses is the maximum allowed by the E.164 numbering plan (up to 15 digits).

The country code (CC) is 1-3 digits.

The National Destination Code (NDC) length depends on the country in question.

The SN is the subscriber number.

The Global Title Indicator is 0010.

The digits of the GTA are coded in Binary Coded Decimal of 1/2 octet per digit.

When the CC is not equal to 1, the E.164 GTA information contains the maximum allowed by the numbering plan. Global Title Translation on 1-3 digits is required to route to the destination country. The output of the final GTT is the DPC and SSN of the destination to which the message is being routed.

B.14.5 Relationship to Existing Application/Translation Groups

Before Number Portability, Translation Type 10 was sufficient for SCCP routing to both PCS1900 MSISDN addresses and PCS1900 NE addresses. With the advent of NP, TT 14 is used for MSISDN addresses and TT 10 is used for NE addresses.

Assignment of a new TT value for this application will not affect other application/translation groups.

B.15 TRANSLATION TYPE CODE VALUE: 00001111 (15)

Application/Translation Group: *Packet Data Interworking*

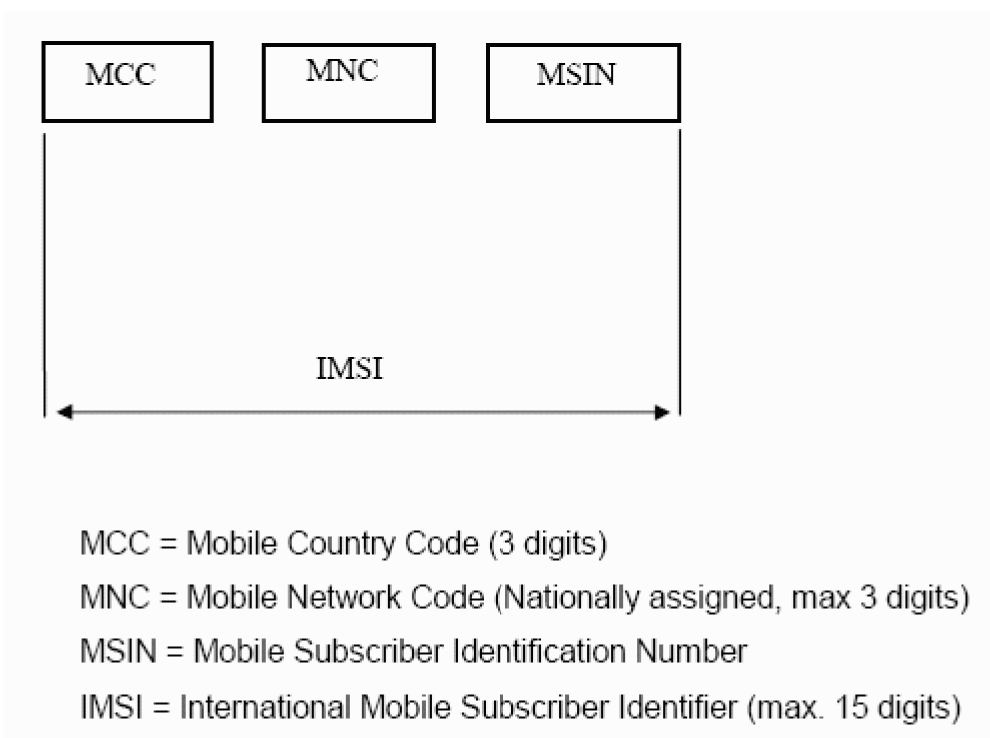
B.15.1 Application Description

With the desire to provide for interoperability between different technology (e.g., GSM and ANSI-136) networks that also support packet data such as General Packet Radio Service (GPRS), the need exists to route to different HLRs based on an IMSI. Normally, TT 9 IMSI to HLR would be used to route to an HLR but when a network has packet data, routing on a single IMSI may need to result in two different destinations: one for TT 9 and one for packet data.

B.15.1.1 IMSI to HLR

When a subscriber roams to a network, the node that will provide service is called a MSC or for packet data the node is the serving system packet node (SSPN) -- e.g., Serving GPRS Service Node (SGSN). In order for the MSC or SSPN to provide service, it must communicate with the appropriate node in the subscriber's home network to inform the home network of the subscriber's location and to retrieve information about the subscriber. The node in the home network is known as the HLR.

The only information available to the serving MSC to allow it to communicate with the subscriber's HLR is the information provided by the subscriber's terminal when it makes contact with the network. This information is in the form of the IMSI and has the format below as defined in the ITU-T Recommendation E.212.



When the MSC receives the IMSI, it uses it to address the subscriber's HLR. This is done by sending a connectionless SCCP message to the HLR using the IMSI as the GT address. Intervening STP's perform GTT to establish the DPC and SSN of the HLR or next translation point.

Note that the IMSI is an E.212 number. It is not a dialable number and does not conform to the E.164 or to the North American Numbering Plan. It is a number used to identify the subscriber within and between wireless networks. It is separate from the number that is dialed when calling the subscriber.

While this translation type is intended for any wireless multi-mode application needing to use a single IMSI to route to different nodes for bearer and packet services, the following is only one specific example of the use of this translation type. In the case of a multi-mode mobile station (e.g., ANSI-136, GSM, and GPRS capable) the following routing cases could occur:

Table B-1/ATIS-1000112.3 - Routing Scenarios Using IMSI to Locate HLR

	Mobile Station Native Mode	Serving Network	Service	SS7 Message		Translation Type (TT)
				Originating Node	Destination Node	
A.	ANSI-136	ANSI-136	Bearer	MSC/VLR	HLR (ANSI)	16
B.	GSM	ANSI-136	Bearer	MSC/VLR	IIF (HLR)*	16
C.	ANSI-136	ANSI-136	Packet	SGSN	GPRS-HLR	15
D.	GSM	ANSI-136	Packet	SGSN	GPRS-HLR	15
E.	ANSI-136	GSM	Bearer	MSC/VLR	IIF (HLR)*	9
F.	GSM	GSM	Bearer	MSC/VLR	HLR (GSM)	9
G.	ANSI-136	GSM	Packet	SGSN	GPRS HLR	15
H.	GSM	GSM	Packet	SGSN	GPRS HLR	15

HLR (ANSI) - The HLR supporting the ANSI-136 system.

HLR (GSM) - The HLR supporting the GSM system.

IIF (HLR) - The Interworking and Interoperability Function (IIF), which performs the protocol conversion and signals to the appropriate HLR using a second process.

GPRS-HLR - the HLR supporting the GPRS data architecture.

SGSN - Serving GPRS Service Node (SGSN).

* A second routing is needed to route from the IIF to the correct HLR as indicated in Table B-2/ATIS-1000112.3.

Table B-2/ATIS-1000112.3 - Secondary Routing Originated by an IIF

	Mobile Station Native Mode	Serving Network	Service	SS7 Message		Translation Type (TT)
				Originating Node	Destination Node	
B´	GSM	ANSI-136	Bearer	IIF	GSM HLR	9
E´	ANSI-136	GSM	Bearer	IIF	ANSI HLR	16

As can be seen from cases B and D, as well as cases E and G, a single IMSI provided by the mobile station results in two different destinations based on the service being invoked by the mobile station. To accommodate this difference, two different translation types are required.

Table B-1/ATIS-1000112.3 provides the multiple routing scenarios when IMSI is used to locate an HLR. Table B-2/ATIS-1000112.3 provides the secondary routing originated by the IIF, which is considered to be equivalent to an SCP.

B.15.2 Internetwork Needs

The internetwork needs defined in this application group require roaming between different wireless (e.g., GSM or ANSI-136) networks, specifically for the applications of Authentication, Registration, and Location Update for all services including packet data.

B.15.3 Involved Nodes

Several types of nodes may be involved in the generation, transport, and reception of messages routed with an E.212 GT address, including:

- HLR, MSC, SSPN (e.g., SGSN), IIF, and SS7 STP's in the home network.
- MSC/VLR, SSPN (e.g., SGSN), IIF, and SS7 STP's of the visited network.
- SS7 STP's of intermediate transport networks.

IIF nodes between different technology networks provide the needed conversions for interworking and interoperability between the two systems.

The following scenario provides one example of such information exchange, where the terminating node (the HLR) is addressed using the E.212 IMSI of the subscriber. While this specific example involves ANSI-136, GSM, and GPRS, it is not intended to limit this translation type. This translation type is for any packet data interworking in a multi-mode environment.

In this scenario, a subscriber from one network has roamed to another network, known as the visited network. When the subscriber registers in the visited network (by powering on the terminal), the MSC/VLR or SGSN (based on service requested) of the visited network obtains the IMSI and uses it as an addressing mechanism to communicate with the HLR in the subscriber's home network.

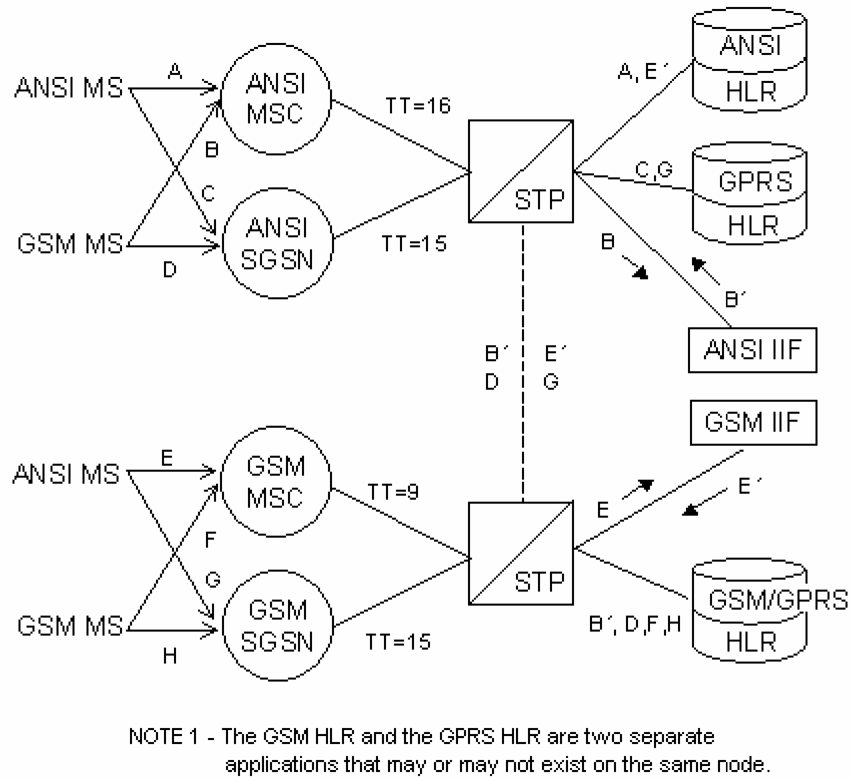


Figure B-17/ATIS-1000112.3 - Involved Nodes for Packet Data Interworking

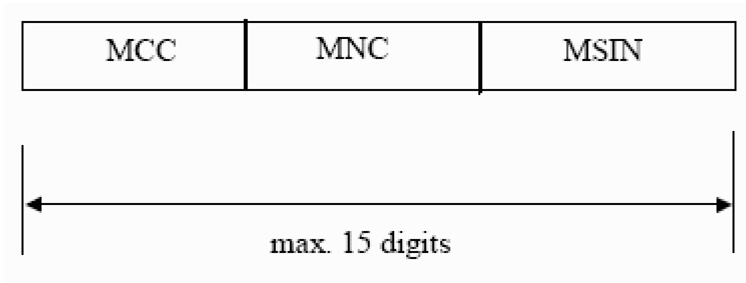
In Figure B-17/ATIS-1000112.3, the mobile station, either GSM native or ANSI-136 native has roamed to a visited network and requests service.

1. Subscriber switches on the mobile station and the subscriber's IMSI (E.212) is transmitted to the MSC/VLR or the SGSN based on the service requested.
2. The MSC/VLR for bearer services generates a connectionless SCCP message and populates the GT address of the called party with the IMSI digits; the TT is set to 9 in GSM networks and set to 16 in ANSI networks. Alternatively, the SGSN for packet data generates a connectionless SCCP message and populates the GT address of the called party with the IMSI digits; the TT is set to "15" to route to the GPRS HLR.
3. Interconnecting SS7 signaling.
4. STP in the home network performs GTT and establishes the DPC and SSN of the appropriate HLR.

The above example shows a case where the subscriber has roamed to another network within North America. It is also possible to roam internationally. Since E.212 is an internationally accepted standard, it can also be used for international roaming.

B.15.4 Global Title Translation Requirements

Global Title Address Information contains an E.212 IMSI number as follows:



MCC = Mobile Country Code (3 digits)

MNC = Mobile Network Code (Nationally assigned, max 3 digits)

The MSIN fills the remaining digits of the GT address.

The GTI is 0010.

The digits of the GT Address are coded in BCD.

When the MCC indicates a North American network, IMSI contains 15 digits. It is expected the first 6 digits will be used to perform the GTT to route to the destination network. It is expected 6 to 10 digits will be used to perform the final GTT.

When the MCC indicates a Non-North American network, IMSI contains 6 to 15 digits. It is expected the first 6 digits will be used to perform the GTT to route outside North America.

B.15.5 Relation to Existing Applications/Translation Groups

There are some similarities between this application and that defined by the TT value 9 *National and International PCS Roaming* (see clause B.9) and the TT=16 *Cellular/PCS Interworking* (see clause B.16) translation type. However, TT value 9 is defined for basic National and International Cellular/PCS Roaming and, as such, does not address the needs of the second destination HLR for packet data when the mobile station is multi-mode. TT=16 only handles the secondary routing from the IIF to the appropriate HLR for bearer service. Neither addresses the needs for packet data services. See Table B-1/ATIS-1000112.3 and Table B-2/ATIS-1000112.3 for a specific example, which provides further details.

This application is not impacted by number portability or number pooling.

B.16 TRANSLATION TYPE CODE VALUE: 00010000

Application/Translation Group: *Cellular/PCS Interworking*

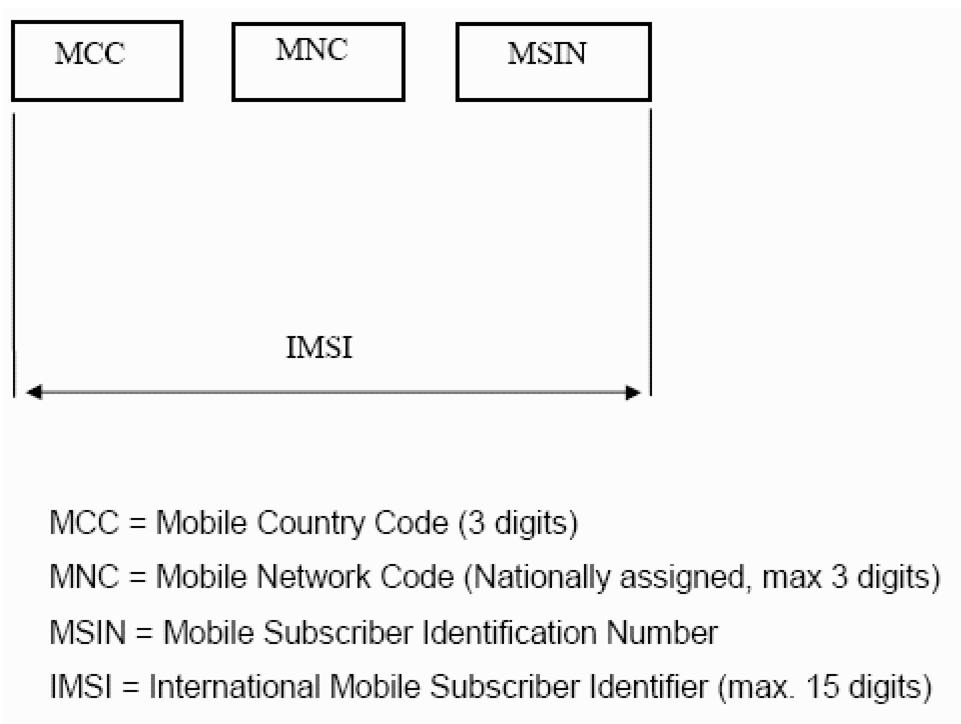
B.16.1 Application Description

With the desire to provide for interoperability and interworking between different technology (e.g., GSM and ANSI-136) networks, the need exists to route to different HLRs and IIFs based on an IMSI. Normally, TT 9 IMSI to HLR would be used to route to an HLR, but when an IIF is introduced to change the protocol messages, routing on a single IMSI needs to result in two different destinations, either IIF or HLR.

B.16.1.1 IMSI to HLR or IIF

When a subscriber roams to a network, the node that will provide service is called an MSC. In order for the MSC to provide service, it must communicate with the appropriate node in the subscriber's home network to inform the home network of the subscriber's location and to retrieve information about the subscriber. The node in the home network is known as the HLR.

The only information available to the serving MSC, to allow it to communicate with the subscriber's HLR is the information provided by the subscriber's terminal when it makes contact with the network. This information is in the form of the IMSI and has the format below as defined in the ITU-T Recommendation E.212.



When the MSC receives the IMSI, it uses it to address the subscriber's HLR. This is done by sending a connectionless SCCP message to the HLR using the IMSI as the GT address. Intervening STP's perform GTT to establish the DPC and SSN of the HLR.

Note that the IMSI is an E.212 number. It is not a dialable number and does not conform to the E.164 or to the North American Numbering Plan. It is a number used to identify the subscriber within and between wireless networks. It is separate from the number that is dialed when calling the subscriber.

While this translation type is intended for any wireless multi-mode application needing to use a single IMSI to route to different nodes for interworking, the following is only one specific example of the use of this translation type. In the case of a multi-mode mobile station (e.g., ANSI-136 and GSM capable) the following routing cases could occur:

Table B-3/ATIS-1000112.3 - Routing Scenarios Using IMSI to Locate HLR

	Mobile Station Native Mode	Serving Network	Service	SS7 Message		Translation Type (TT)
				Originating Node	Destination Node	
A.	ANSI-136	ANSI-136	Bearer	MSC/VLR	HLR (ANSI)	16
B.	GSM	ANSI-136	Bearer	MSC/VLR	IIF (HLR)*	16
E.	ANSI-136	GSM	Bearer	MSC/VLR	IIF (HLR)*	9
F.	GSM	GSM	Bearer	MSC/VLR	HLR (GSM)	9

HLR (ANSI) - The HLR supporting the ANSI-136 system.

HLR (GSM) - The HLR supporting the GSM system.

IIF (HLR) - The Interworking and Interoperability Function (IIF), which performs the protocol conversion and signals to the appropriate HLR using a second process.

GPRS-HLR - the HLR supporting the GPRS data architecture.

SGSN - Serving GPRS Service Node (SGSN).

* A second routing is needed to route from the IIF to the correct HLR as indicated in Table B-4/ATIS-1000112.3.

Table B-4/ATIS-1000112.3 - Secondary Routing Originated by an IIF

	Mobile Station Native Mode	Serving Network	Service	SS7 Message		Translation Type (TT)
				Originating Node	Destination Node	
B´	GSM	ANSI-136	Bearer	IIF	GSM HLR	9
E´	ANSI-136	GSM	Bearer	IIF	ANSI HLR	16

Table B-3/ATIS-1000112.3 provides the multiple routing scenarios when IMSI is used to locate an HLR. Table B-4/ATIS-1000112.3 provides the secondary routing originated by the IIF, which is considered to be equivalent to an SCP. In each case where a message is routed to the IIF, the message is then converted from one protocol (GSM or ANSI-41) to the other. A new message is originated by the IIF in the new protocol using TT 16 to route to the ANSI-136 HLR or TT 9 to route to the GSM HLR. This means that a single IMSI is used to route one message to the IIF and the same IMSI is used in another message to route to the appropriate HLR. See Table B-4/ATIS-1000112.3 for additional information.

Table B-5/ATIS-1000112.3 - Use of TT9 and TT16 to Differentiate Routing to an IIF from an HLR

Serving Network	Translation Type	IMSI range	Destination
GSM	9	GSM	GSM HLR
ANSI-136	16	GSM	IIF
GSM	9	ANSI-136	IIF
ANSI-136	16	ANSI-136	ANSI-136 HLR
GSM (IIF)	16	ANSI-136	ANSI-136 HLR
ANSI-136 (IIF)	9	GSM	GSM HLR

This new translation type and its use in the ANSI-136 networks allows one STP pair to serve both types of networks, and a single IIF to be served by only one STP. Note that the IIF involves more than simple mapping between protocols and may need to store information not sent in the new message. It must also keep an open transaction pending a return response when appropriate.

B.16.2 Internetwork Needs

The internetwork needs defined in this application group require roaming between different technology networks, specifically for the applications of Authentication, Registration, and Location Update for all services.

B.16.3 Involved Nodes

Several types of nodes may be involved in the generation, transport, and reception of messages routed with an E.212 GT address, including:

- HLR, MSC, IIF, and SS7 STP’s in the home network.
- MSC/VLR, IIF, and SS7 STP’s of the visited network.
- SS7 STP’s of intermediate transport networks.
- IIF nodes between technology networks provide for the needed conversions for interworking and interoperability between the two systems.

The following scenario provides an example of such information exchange, where the terminating node (the HLR) is addressed using the E.212 IMSI of the subscriber. While this specific example involves ANSI-136 and GSM, it is not intended to limit this translation type. This translation type is for any inter-technology interworking in a multi-mode environment.

In this scenario, a subscriber from one network has roamed to another network, known as the visited network. When the subscriber registers in the visited network (by powering on the terminal), the MSC/VLR of the visited network obtains the IMSI and uses it as an addressing mechanism to communicate with the HLR in the subscriber’s home network.

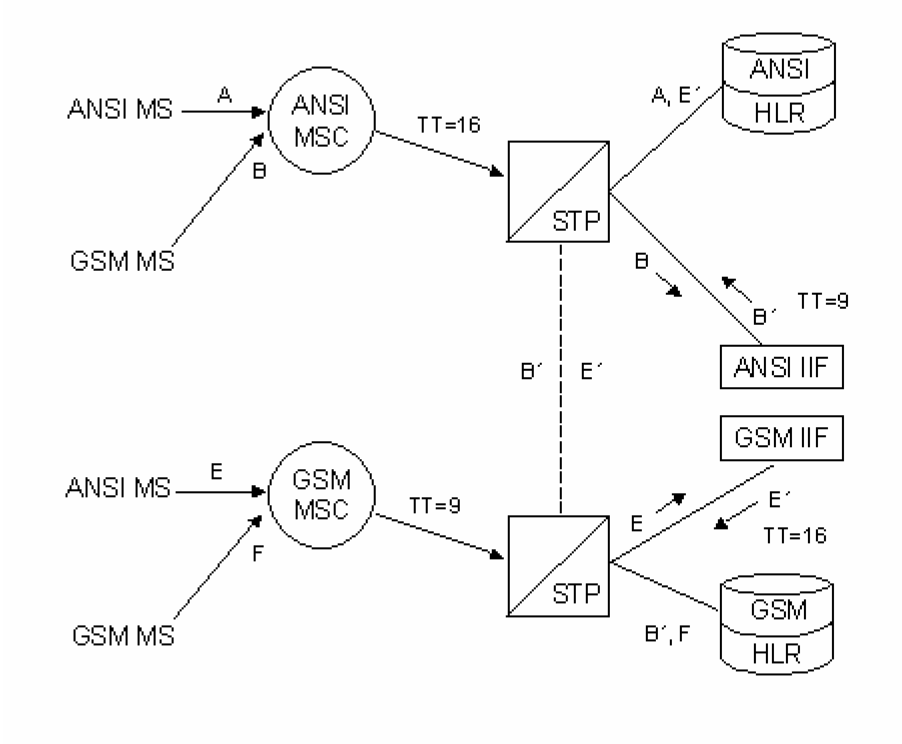


Figure B-18/ATIS-1000112.3 - Involved Nodes for GSM/ANSI-136 Interworking

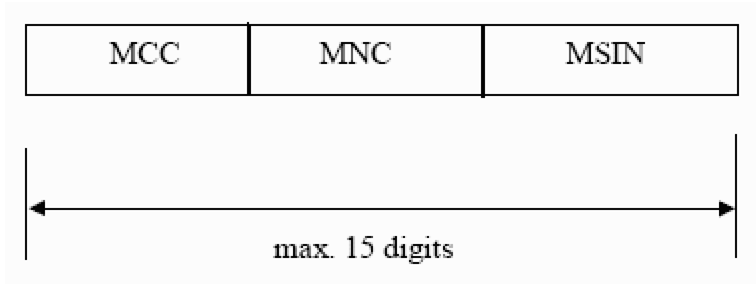
In Figure B-18/ATIS-1000112.3, the mobile station, either GSM native or ANSI-136 native has roamed to a visited non-native network and requests service.

1. Subscriber switches on the mobile station and the subscriber's IMSI (E.212) is transmitted to the MSC/VLR.
2. The MSC/VLR for bearer services generates a connectionless SCCP message and populates the GT address of the called party with the IMSI digits; the TT is set to 9 in GSM networks and in ANSI-136 networks the TT is set to 16.
3. Interconnecting SS7 signaling.
4. STP in the serving network performs GTT and establishes the DPC and SSN of the IIF. The IIF then converts the message from the visited network protocol to the native mode protocol and sends a new message to the native mode HLR, setting the TT to 16 to route to ANSI-136 HLRs or TT to 9 to route to GSM HLRs.

The above specific example shows a case where the subscriber has roamed to another network within North America. It is also possible to roam internationally. Since E.212 is an internationally accepted standard, it can also be used for international roaming.

B.16.4 Global Title Translation Requirements

Global Title Address Information contains an E.212 IMSI number as follows:



MCC = Mobile Country Code (3 digits)

MNC = Mobile Network Code (Nationally assigned, max 3 digits)

The MSIN fills the remaining digits of the GT address.

The GTI is 0010.

The digits of the GT Address are coded in BCD.

When the MCC indicates a North American network, IMSI contains 15 digits. It is expected the first 6 digits will be used to perform the GTT to route to the destination network. It is expected 6 to 10 digits will be used to perform the final GTT.

When the MCC indicates a Non-North American network, IMSI contains 6 to 15 digits. It is expected the first 6 digits will be used to perform the GTT to route outside North America.

B.16.5 Relation to Existing Applications/Translation Groups

There are some similarities between this application and that defined by the TT value 9 *National and International PCS Roaming* (see clause B.9). However, TT value 9 is defined for basic National and International Cellular/PCS Roaming and, as such, does not address the needs of the second destination when routing out of the IIF. See Tables B-3/ATIS-1000112.3, B-4/ATIS-1000112.3, and B-5/ATIS-1000112.3 for a specific example that provides further details.

This application is not impacted by number portability or number pooling.

B.17 TRANSLATION TYPE CODE VALUE: 00010001 (17)

Application/Translation Group: *Mobile Subscriber Message Center Addressing*

B.17.1 Application Description

This application is used for routing a Mobile Directory Number (MDN) to a MC. TT 14 MDN to HLR is used to route to a HLR. TT 10 E.164 to Network Entity is used to route to a network entity. The E.164 numbers used in TT 10 are not considered portable.

In the ANSI-41 network a mobile subscriber who wants to send a short message to another mobile subscriber addresses the message to the MDN. The message from the originating subscriber is sent to the originator's MC using the MIN or IMSI for the Global Title Address with TT 12 or 13 respectively. Prior to deployment of NP, the MDN and MIN were the same in North America. The originator's MC would use the MDN as the MIN to send the message to the Terminating subscriber's MC using the TT 12.

Following the deployment of NP the MDN may no longer be the same as the MIN. This requires that the network now route the short message to the terminating subscriber's MC based on an MDN that is different than the MIN. Also to support international roaming and delivery of short messages to international mobile subscribers, the MDN needs to be a full E.164 number.

B.17.2 Internetwork Needs

The internetwork needs defined in this application group require roaming between different wireless networks, specifically for the application of SMS from an MC in one network to an MC in another network using an MDN as the global title in an SCCP called party address.

B.17.3 Involved Nodes

The following types of node may be involved in the reception and transport of Short Messages routed to an MC based on the MDN:

- *Originating Node*: MC or MSC
- *Transport Node*: STP or NP GTT function
- *Destination Node*: MC

The originating Node assigns this translation type when it wishes to route to a destination MC and the SCCP called party address contains an MDN. Initial routing and transport by STP's is based on SCCP GTT of the first seven digits (country code "1" plus NPA-NXX) of the MDN in the SCCP called party address. The STP translation may give the signaling point code of the destination MC, another STP, or an NP GTT function (which may be the STP itself). Routing to an NP GTT function may occur for an MDN that lies in a portable NPA-NXX range if the STP has an arrangement with an NP GTT serving this portable NPA-NXX. Transport by the NP GTT function shall occur when it is necessary to perform eleven digits SCCP GTT on an MDN lying within a portable NPA-NXX range.

The following scenario provides an example of sending a short message from an originating MC to a Terminating MC where both networks have an arrangement to use a transit network.

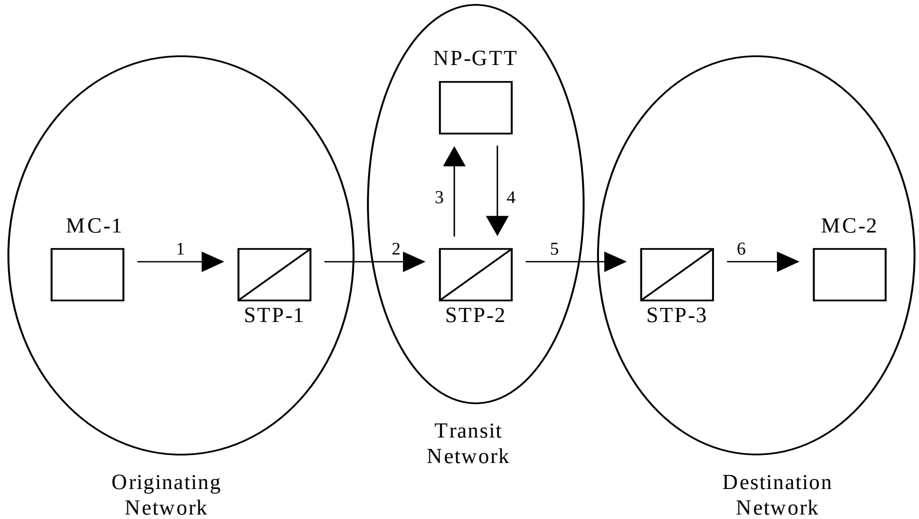


Figure B-19/ATIS-1000112.3 - Involved Nodes for Short Message Transfer

1. The originating MC-1 responsible for delivering a short message to some terminating mobile subscriber's MC sends the short message towards the destination MC of this subscriber. This message contains the MDN of the subscriber in the global title of the SCCP called party address. The translation type for this address is TT '17'. The message is MTP routed initially to STP-1 in the same network.
2. STP-1 translates the country code “1” and NPA-NXX portion of the SCCP MDN address. The translation result is the signaling point code of STP-2 to which the message is then MTP routed.
3. STP-2 translates the country code “1” and NPA-NXX portion of the SCCP MDN address. Because the NPA-NXX is portable, the translation result is the signaling point code of a GTT NP function. If the NPA-NXX was not portable, it would be unnecessary to route to an NP GTT function, and the translation result could be the signaling point code of STP-3: in this case, routing steps 3 and 4 to the NP GTT would be omitted.
4. The NP-GTT function translates the country code “1” and entire NPA-NXX-XXXX digits of the SCCP MDN address. The translation result is the signaling point code of STP-3. The message is MTP routed to STP-2.
5. STP-2 MTP routes the message to STP-3.
6. STP-3 performs final GTT and routes the message to the MC-2. Note that final GTT could be performed in the transit network if the destination network has such an agreement.

The following scenario provides an example of sending a short message from an Originating MC to a Terminating MC where the networks have a direct signaling connection:

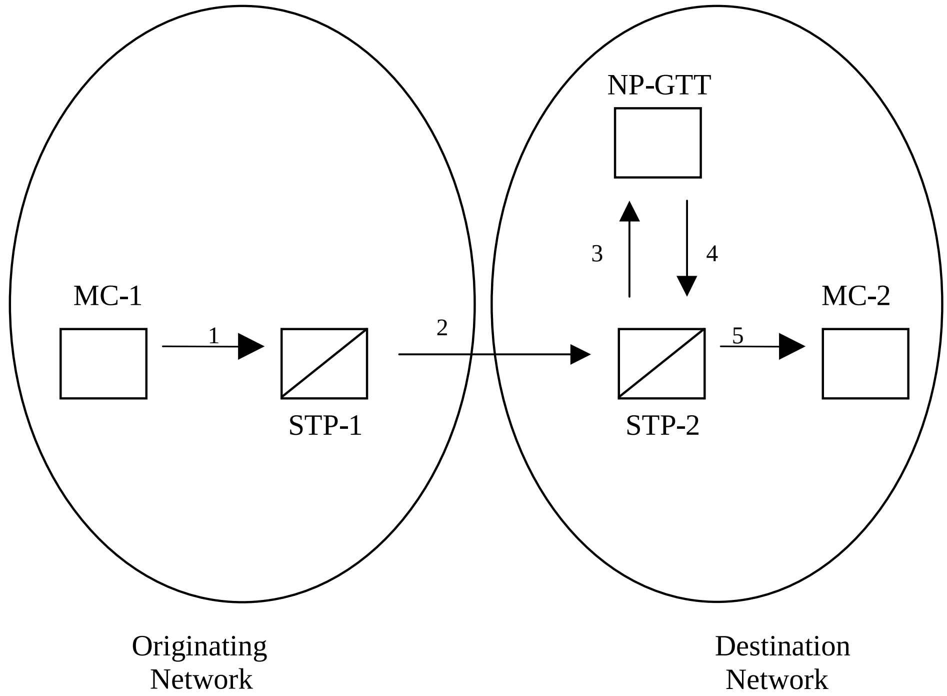
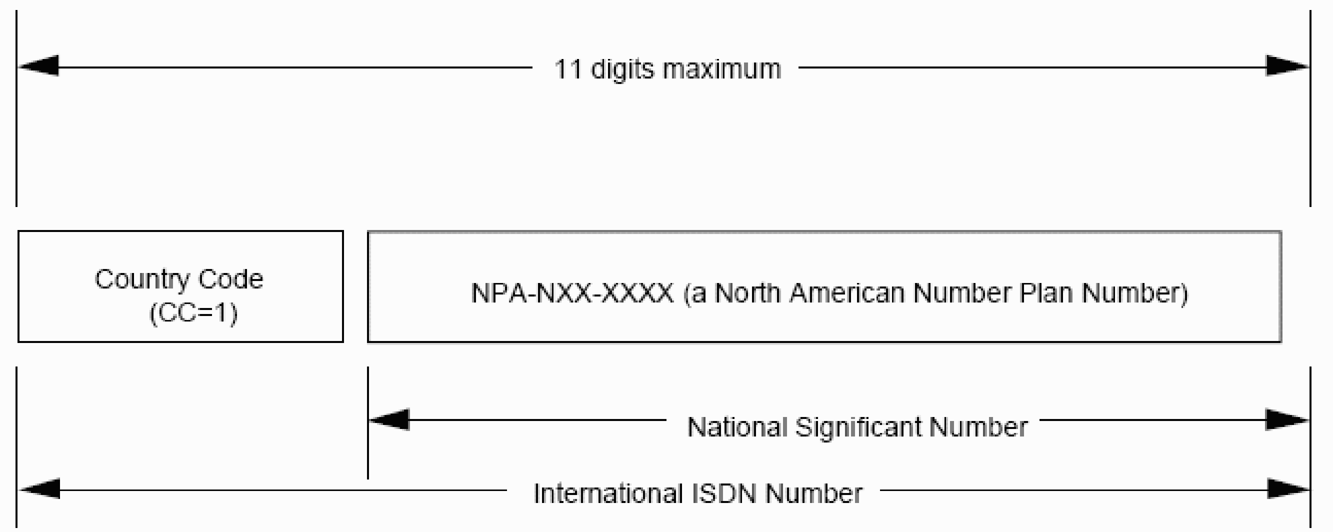


Figure B-20/ATIS-1000112.3 - Involved Nodes for Short Message Transfer

1. The originating MC-1 responsible for delivering a short message to some terminating mobile subscriber's MC sends the short message towards the destination MC of this subscriber. This message contains the MDN of the subscriber in the global title of the SCCP called party address. The translation type for this address is TT '17'. The message is MTP routed initially to STP-1 in the same network.
2. STP-1 translates the country code “1” and NPA-NXX portion of the SCCP MDN address. The translation result is the signaling point code of STP-2 to which the message is then MTP routed.
3. STP-2 translates the country code “1” and NPA-NXX portion of the SCCP MDN address. Because the NPA-NXX is portable, the translation result is the signaling point code of a GTT NP function. If the NPA-NXX was not portable, it would be unnecessary to route to an NP GTT function, and the translation result could be the signaling point code of MC-2: In this case, routing steps 3 and 4 to the NP GTT would be omitted.
4. The NP-GTT function translates the country code “1” and entire NPA-NXX-XXXX digits of the SCCP MDN address. The translation result is the signaling point code MC-2. The message is MTP routed to STP-2.
5. STP-2 MTP routes the message to MC-2.

B.17.4 Global Title Translation Requirements

The format of the MDN address in the GTA is based on the E.164 numbering plan. For Integrated Numbering Plan with CC=1, the format is shown below:



E.164 Number Format for CC=1

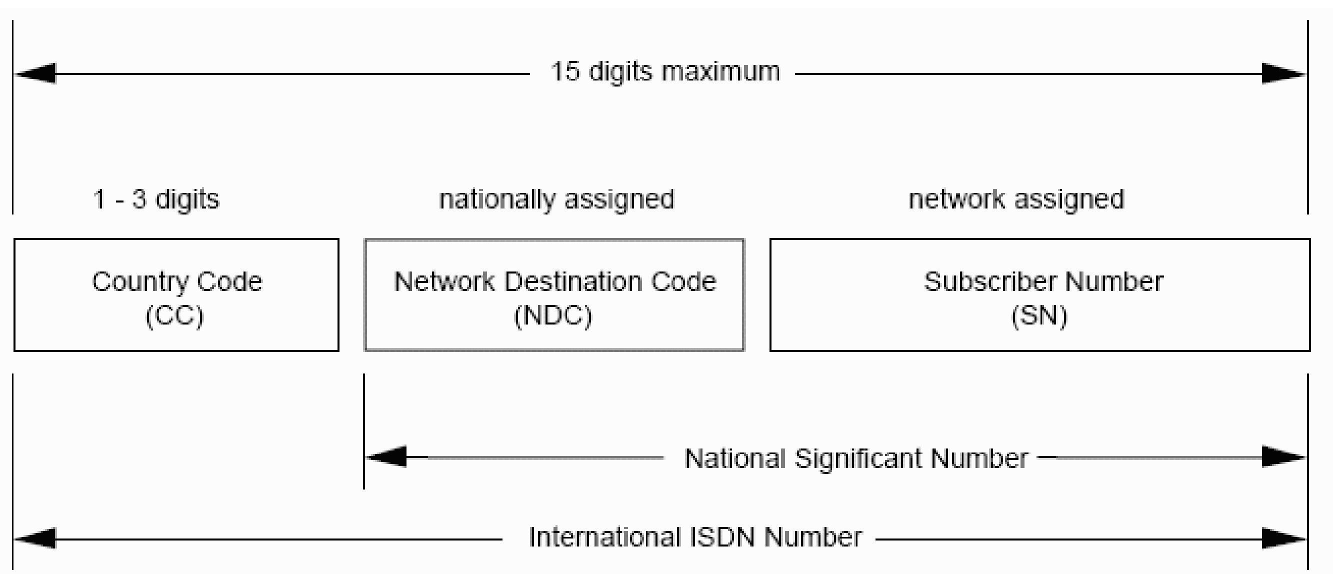
When CC=1, the maximum length of the E.164 GTA is 11 digits.

The GTI is 0010.

The digits of the GTA are BCD in 1/2 octet per digit.

When CC=1, the MDN in the E.164 GTA contains 11 digits. GTT on the first seven digits is required to route to the boundaries (defined by GTT databases) of an area of portability. Within the area of portability, an eleven-digit GTT is required for delivery to the final destination network. The output of the final GTT is the DPC and SSN of the destination to which the message is being routed.

When the CC is not equal to 1, the format of the E.164 GTA is as shown below:



E.164 Number Format For Other Than CC=1

The maximum length of the GTA information for other than CC=1 is the maximum allowed by the E.164 numbering plan (up to 15 digits).

The country code (CC) is 1 to 3 digits.

The NDC length depends on the country in question.

The SN is the subscriber number.

The GTI is 0010.

The digits of the GTA are coded in BCD of 1/2 octet per digit.

When the CC is not equal to 1, the E.164 GTA information contains the maximum allowed by the numbering plan. GTT on 1 to 3 digits is required to route to the destination country. The output of the final GTT is the DPC and SSN of the destination to which the message is being routed.

B.17.5 Relation to Existing Applications/Translation Groups

The relationship between this application and that defined by the TT value 10 *Network Entity Routing* (see clause B.10) is that TT 10 is used to route responses to network entities (based on E.164 addresses not considered to be portable). This application group is used for routing to a subscriber's short message MC. The relationship between this application and the TT=14 *Mobile Subscriber Addressing* (see clause B.14) is that TT 14 is routing to a mobile subscriber's HLR and this translation type is routing to the mobile subscriber's MC. All 3 of these translation types are needed for any given MDN to be able to do call delivery to an MDN's HLR that may be portable, routing to a network entity based on a non portable E.164 address, and routing to an MDN's MC that may be portable.

B.18 TRANSLATION TYPE CODE VALUE: 00010010 (18)

Application/Translation Group: *ECS Call Routing*

B.18.1 Application Description

Emergency Calling Service (ECS) allows emergency service calls to be completed through the network to an appropriate emergency service attendant, and to provide the PSAP attendant with location information (if available) regarding the calling user. ECS supports other capabilities such as priority routing of the call within the network, and transfer of emergency calls to other attendants. ECS Call Routing can either be handled completely within a switching system, or by querying an external database. If an external database is used, ECS call routing can be accomplished by using TCAP messaging to retrieve the necessary call routing information. GTTs are performed at one or more STPs to identify the network node that contains the ECS call routing information for emergency calls being processed by a particular emergency service routing exchange.

B.18.2 Internetwork Needs

Internetwork messaging will occur when the network in which the database containing ECS call routing information resides is different from the network in which the switch that is processing the emergency call resides, and appropriate arrangements exist between network providers to allow querying of the ECS call routing database by other networks. For this reason, an internetwork Translation Type code value is required.

B.18.3 Involved Nodes

The SEP processing the emergency call generates a TCAP query message which requires GTT routing at one or more STPs. This query message is ultimately routed to the ECS call routing database (i.e., Selective Routing Database [SRDB]) associated with the geographic area in which the emergency call originated. Figure B21/ATIS-1000112.3 is an ECS Call Routing example diagram.

B.18.3 Involved Nodes

The SEP processing the emergency call generates a TCAP query message which requires GTT routing at one or more STPs. This query message is ultimately routed to the ECS call routing database (i.e., Selective Routing Database [SRDB]) associated with the geographic area in which the emergency call originated. Figure B21/ATIS-1000112.3 is an ECS Call Routing example diagram.

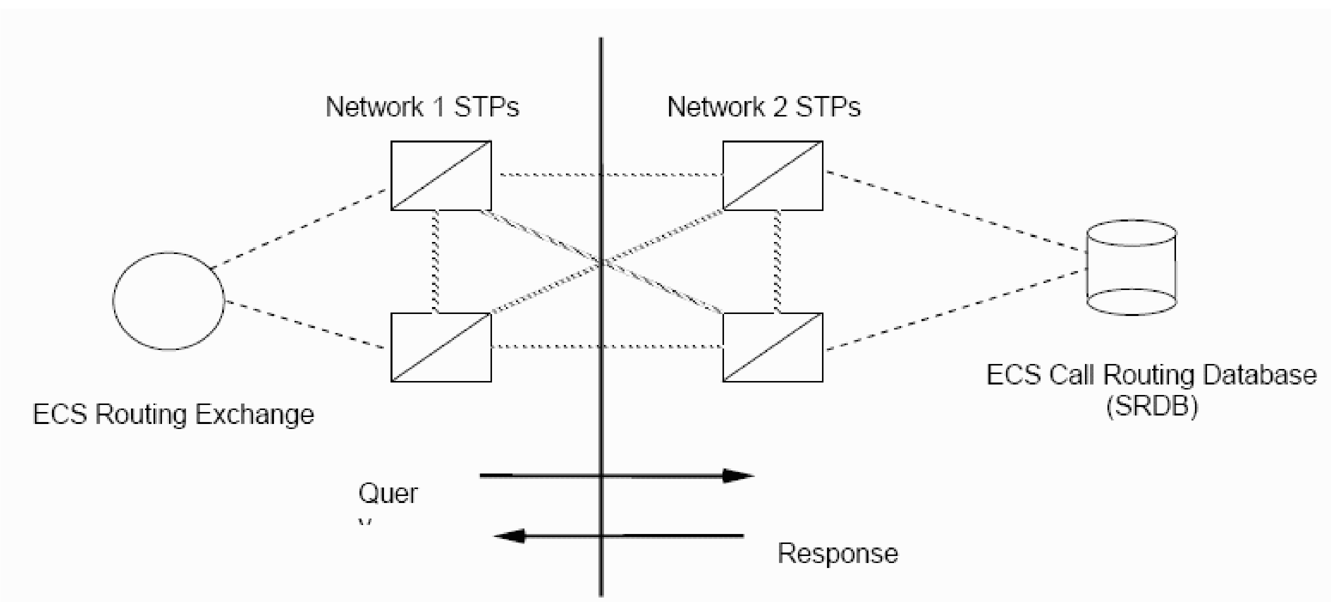


Figure B-21/ATIS-1000112.3 – ECS Call Routing Example Diagram

B.18.4 Global Title Translation Requirements

The Global Title Address information will contains the first six digits of a 10-digit North American Numbering Plan (NANP) number in the format of NPA+NXX-XXXX, associated with the switch that is originating the ECS call routing query. If the switch supports Number Portability, the Global Title Address will contain the NPA-NXX-XXXX of a Location Routing Number that is associated with the switch launching the query. If the switch that is originating the ECS call routing query does not support Number Portability, the Global Title Address will contain a representative NPA-+NXX-XXXX that is associated with the switch. The Global Title Address information is encoded as BCD. Global Title Indicator type 2 will be used.

It is expected that either 3 or 6-10 digits of the Global Title Address information will be used for GTT. The output of the final GTT will be the point code and SSN of the database where the ECS call routing data is stored.

B.18.5 Relationship to Existing Application/Translation Groups

The Global Title Address information in this application/translation group is similar to other existing groups, however, this application requires independently allocated resources and management (i.e., the output of the global title translation must be the SRDB).

B.28 TRANSLATION TYPE CODE VALUE: 00011110 (28)

Application/Translation Group: *14 Digit Telecommunications Calling Cards - Post-10-digit (NP) GTT*

B.28.1 Application Description

The introduction of Number Portability impacts the routing of TCAP queries related to the 14 Digit Telecommunications Calling Cards application, but does not affect the application itself. Therefore, the Application Description associated with the Application/Translation Group "14 Digit Telecommunications Calling Cards - Post-10-digit (NP) GTT" is identical to the Application Description associated with the 14 Digit Telecommunications Calling Cards Application/Translation Group. See clause B.2 for a detailed description of the 14 Digit Telecommunications Calling Cards application.

The 14 Digit Format Telecommunications Calling Card will be used for:

- ♦ Payment of the telephone charge;
- ♦ Service charges due; and
- ♦ Validation procedures

to a 14 digit format telecommunications calling card database. This service requires a different database than the 891 telecommunications calling card database.

B.28.2 Internetwork Needs

When the 14 Digit Format Telecommunications Calling Card is used outside of its card issuing network, then internetwork messaging occurs. Internetwork routing of 14 Digit Telecommunications Calling Card queries will be impacted by NP. In an NP environment, some 14 Digit Telecommunications Calling Card queries will have to undergo a 10-digit (NP) GTT function to determine the true destination network for the query. To prevent looping of messages by allowing a subsequent network to identify the query as one which has already undergone 10-digit (NP) GTT processing, an internetwork Translation Type code is required.

B.28.3 Involved Nodes

With the introduction of Number Portability, 14 digit Calling Card queries may traverse an NP GTT node where a 10-digit translation will be performed to identify the destination network for the query[20]. The NP GTT node will be responsible for ensuring that the output Global Title information is as described herein. Subsequent nodes will receive the new Global Title information. This information will be used in any subsequent GTTs used to route the message to the 14 Digit database. See Figure B-21/ATIS-1000112.3.

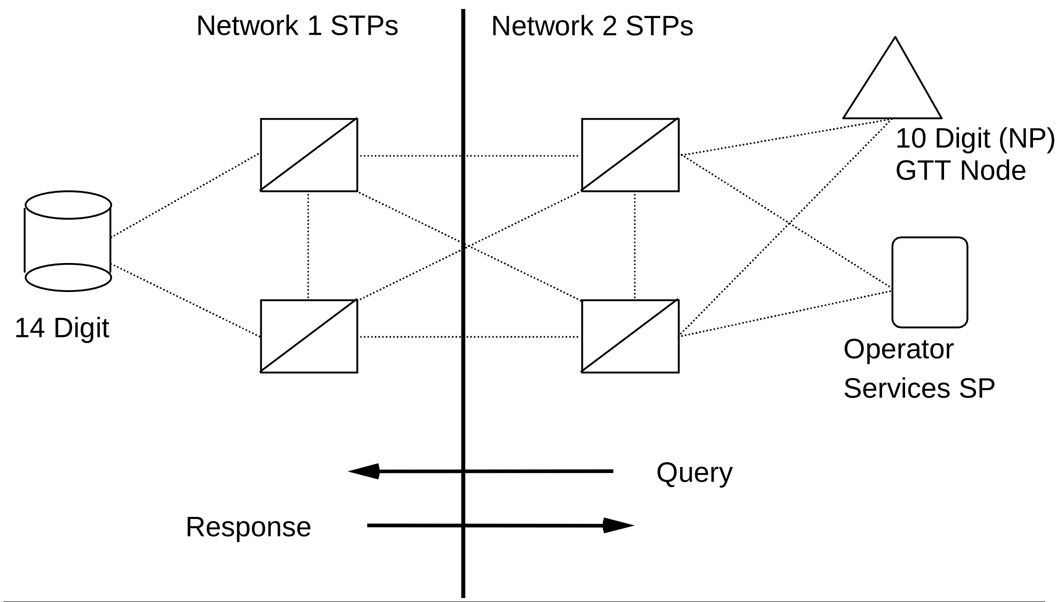


Figure B-22/ATIS-1000112.3 - NP 14 Digit Telecommunications Calling Card Example Diagram

B.28.4 Global Title Translation Requirements

B.28.4.1 Format of 14 Digit Telecommunications Calling Card

Format: NPA NXX XXXX XXXX where:

- NPA is a valid NPA approved by the North American Number Plan Administrator
- N can be any digit from 2-9
- X can be any digit from 0-9

[20] Note that the global title address information contained in a query associated with the 14 Digit Format Telecommunications Calling Card Application, as currently described in clause B.2, will consist of six digits. If the global title address information in a query received by the 10-digit (NP) GTT function consists of less than ten digits, the 10-digit (NP) GTT function will obtain ten digits of information from the relevant parameter within the data field of the query and perform a 10-digit translation on that information.

Special Billing Format[21]:

CIID: NXXWXX XXXX NXXX where:

- N can be any digit from 2-9
- X can be any digit from 0-9
- W can be any digit from 0-1
- NXXWXX is the car issuer ID
- XXXX is the customer account
- NXXX is the personal identification number (non-visible)

RAO: XXX XXXXXXXXXXX where:

- X can be any digit of the form 0-9; and
- XXX is the RAO
- XXXXXXXXXXX is the customer identification number

B.28.4.2 Global Title Translation Addressing Information

After a 10-digit (NP) GTT is performed, a translation will be performed at a subsequent GTT node. The global title address information takes one of the following two forms.

1. When the subsequent GTT node supports translation of ported numbers for this translation type, address information is the first six or ten digits of the 14-digit Telecommunications Calling Card number.
2. [Optionally by network] When the subsequent GTT node does not support translation of ported numbers for this translation type, the address information is either:
   a. The first six or ten digits of the 14-digit Telecommunications Calling Card number when the number is not ported.
   b. A routing number, supplied by the 10-digit (NP) GTT function, when the NANP number on the calling card is ported.

This information is encoded as BCD. Global Title Indicator type 2 will be used. It is expected that either the first 3, 6, or 10 digits of the global title address information will be used to perform the final GTT. The output of the final GTT will be the point code and SSN of the 14-Digit Calling Card database.

B.28.5 Relationship to Existing Application/Translation Groups

This application is very similar to the 14 Digit Telecommunications Calling Cards Application Group, but translation requirements are different due to the impacts of Number Portability on the routing of 14-Digit Telecommunication Calling Card queries. This application/translation group provides a mechanism to prevent looping.

---

[21] Since special billing formats are not subject to Number Portability, it is expected that queries related to calling cards that use these formats will not interact with the 10-digit (NP) GTT function and will, therefore, continue to use the existing 14 Digit Telecommunications Calling Card format, as specified in clause B.2.

B.29 TRANSLATION TYPE CODE VALUE: 29

Application/Translation Group: *Calling Name Delivery - Post-10-digit (NP) GTT*

B.29.1 Application Description

The introduction of NP impacts the routing of TCAP queries related to the Calling Name Delivery application, but does not affect the application itself. Therefore, the Application Description associated with the Application/Translation Group "Calling Name Delivery - Post-10-digit (NP) GTT" is identical to the Application Description associated with the Calling Name Delivery Application/Translation Group. See clause B.5 for a detailed description of the Calling Name Delivery application.

B.29.2 Internetwork Needs

In the future, when a calling party in one network calls a CNAM subscriber in another network, internetwork messaging will occur during the retrieval of the calling party name information from the calling party's associated database. Internetwork routing of CNAM queries will be impacted by NP. In an NP environment, some CNAM queries will have to undergo a 10-digit (NP) GTT function to determine the true destination network for the query. To prevent looping of messages by allowing a subsequent network to identify the CNAM query as one which has already undergone 10-digit (NP) GTT processing, an internetwork Translation Type code is required.

B.29.3 Involved Nodes

With the introduction of Number Portability, CNAM queries may traverse an NP GTT node where a 10-digit translation will be performed to identify the destination network for the query. The NP GTT node will be responsible for ensuring that the output Global Title information is as described herein. Subsequent nodes will receive the new Global Title information. This information will be used in any subsequent GTTs used to route the message to the Calling Name database associated with the calling party. See Figure B-22/ATIS-1000112.3.

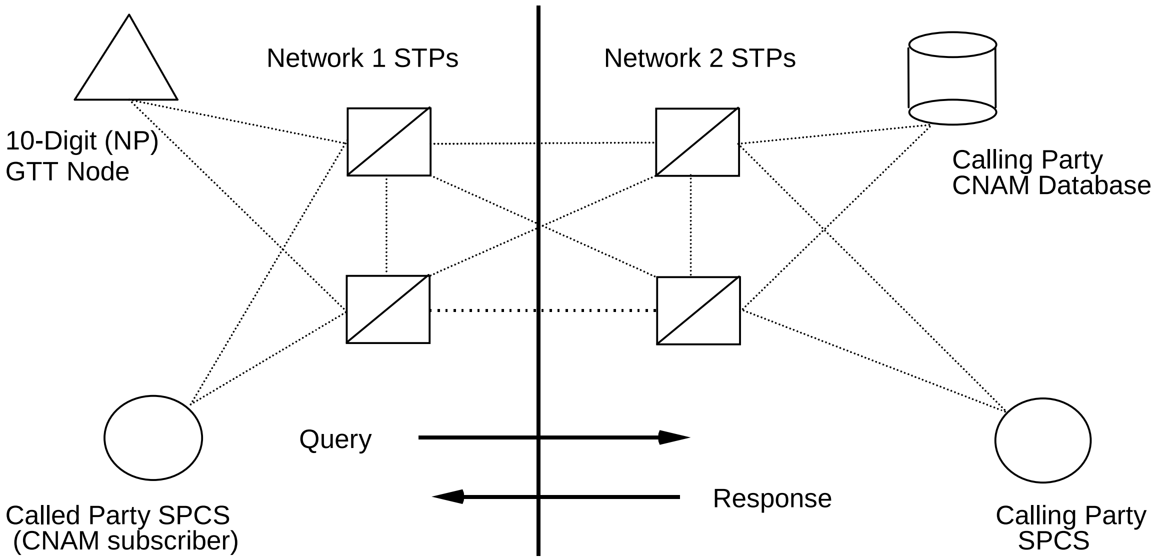


Figure B-23/ATIS-1000112.3 - NP Calling Name Delivery Example Diagram

B.29.4 Global Title Translation Requirements

After a 10-digit (NP) GTT is performed, a translation will be performed at a subsequent GTT node. The global title address information takes one of the following two forms.

1. When the subsequent GTT node supports translation of ported numbers for this translation type, address information is the ten digit calling number.
2. [Optionally by network] When the subsequent GTT node does not support translation of ported numbers for this translation type, the address information is either:
   a. The ten digit calling number when the number is not ported.
   b. A routing number, supplied by the 10-digit (NP) GTT function, when the ten digit calling number is ported.

This information is encoded as BCD. Global Indicator type 2 will be used. Either the first 3, 6, or 10 digits of the global title address information will be sufficient to perform the final GTT. The output of the final GTT will be the point code and SSN of the database where calling name information is stored.

B.29.4.1 Relationship to Existing Application/Translation Groups

This application is very similar to the Calling Name Delivery application group, but translation requirements are different due to the impacts of Number Portability on the routing of CNAM queries. This application/translation group provides a mechanism to prevent looping.

B.30 TRANSLATION TYPE CODE VALUE: 30

Application/Translation Group: *Call Management - Post-10-digit (NP) GTT*

B.30.1 Application Description

The introduction of Number Portability impacts the routing of TCAP queries related to the Call Management application, but does not affect the application itself. Therefore, the Application Description associated with the Application/Translation Group "Call Management - Post-10-digit (NP) GTT" is identical to the Application Description associated with the Call Management Application/Translation Group. See clause B.6 for a detailed description of the Call Management application.

B.30.2 Internetwork Needs

In the future, when a Call Management subscriber in one network communicates with another network, internetwork TCAP messaging will occur as queries and responses are sent (e.g., to determine line status). Internetwork routing of queries related to Call Management services will be impacted by NP. In an NP environment, some queries will have to undergo a 10-digit (NP) GTT function to determine the true destination network for the query. To prevent looping of messages by allowing a subsequent network to identify the Call Management-related query as one which has already undergone 10-digit (NP) GTT processing, an internetwork Translation Type code is required.

B.30.3 Involved Nodes

With the introduction of Number Portability, Call Management queries may traverse an NP GTT node where a 10-digit translation will be performed to identify the destination network for the query. The NP GTT node will be responsible for ensuring that the output Global Title information is as described herein. Subsequent nodes will receive the new Global Title information. This information will be used in any subsequent GTTs used to route the message to node serving the Call Management application. See Figure B-23/ATIS-1000112.3.

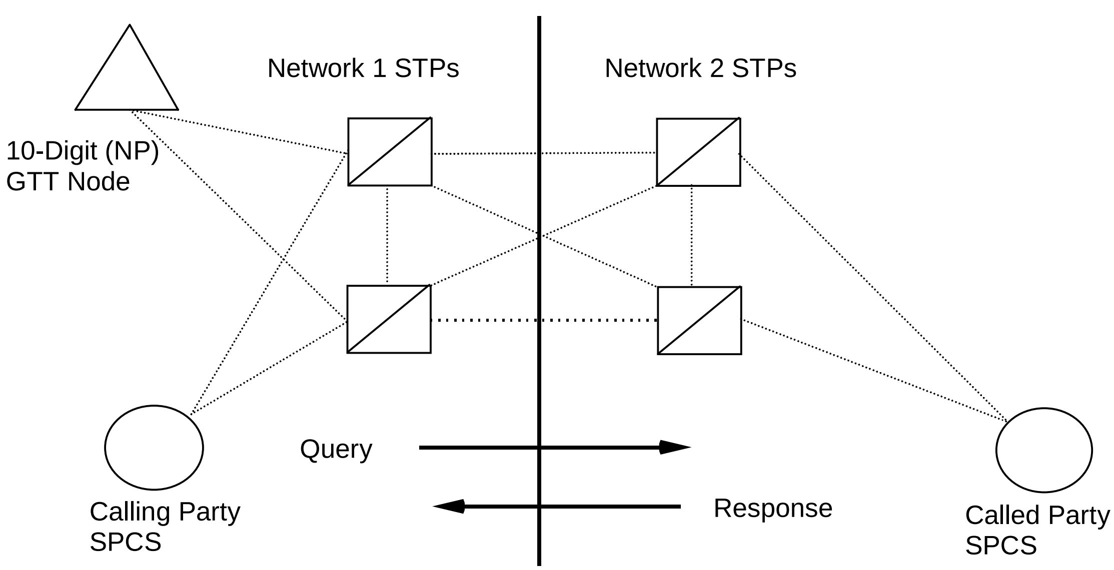


Figure B-24/ATIS-1000112.3 - NP Call Management Example Diagram

B.30.4 Global Title Translation Requirements

After a 10-digit (NP) GTT is performed, a translation will be performed at a subsequent GTT node. The global title address information takes one of the following two forms:

1. When the subsequent GTT node supports translation of ported numbers for this translation type, address information is the ten digit called number.
2. [Optionally by network] When the subsequent GTT node does not support translation of ported numbers for this translation type, the address information is either:
   a. The ten digit called number when the number is not ported.
   b. A routing number, supplied by the 10-digit (NP) GTT function, when the called number is ported.

This information is encoded as BCD. Global Title Indicator type 2 will be used. Either the first 3, 6, or 10 digits of the global title address information will be sufficient to perform the GTT. The output of the final GTT will be the point code of the SEP serving the Called Party and the SSN of the application.

B.30.5 Relationship to Existing Application/Translation Groups

This application is very similar to the Call Management application group, but translation requirements are different due to the impacts of Number Portability on the routing of Call Management queries. This application/translation group provides a mechanism to prevent looping.

B.31 TRANSLATION TYPE CODE VALUE: 31

Application/Translation Group: *Message Waiting - Post-10-digit (NP) GTT*

B.31.1 Application Description

The introduction of NP impacts the routing of TCAP queries related to the Message Waiting application, but does not affect the application itself. Therefore, the Application Description associated with the Application/Translation Group "Message Waiting - Post-10-digit (NP) GTT" is identical to the Application Description associated with the Message Waiting Application/Translation Group. See clause B.7 for a detailed description of the Message Waiting application.

B.31.2 Internetwork Needs

In the future, when an MSS in one network communicates with a Message Waiting subscriber in another network to modify the subscriber's Message Waiting indicator, internetwork TCAP messaging will occur. Internetwork routing of queries related to Message Waiting services will be impacted by NP. In an NP environment, some queries will have to undergo a 10-digit (NP) GTT function to determine the true destination network for the query. To prevent looping of messages by allowing a subsequent network to identify the Message Waiting query as one which has already undergone 10-digit (NP) GTT processing, an internetwork Translation Type code is required.

B.31.3 Involved Nodes

With the introduction of NP, Message Waiting queries may traverse an NP GTT node where a 10-digit translation will be performed to identify the destination network for the query. The NP GTT node will be responsible for ensuring that the output Global Title information is as described herein. Subsequent nodes will receive the new Global Title information. This information will be used in any subsequent GTTs used to route the message to node serving the Call Management application. See Figure B-24/ATIS-1000112.3.

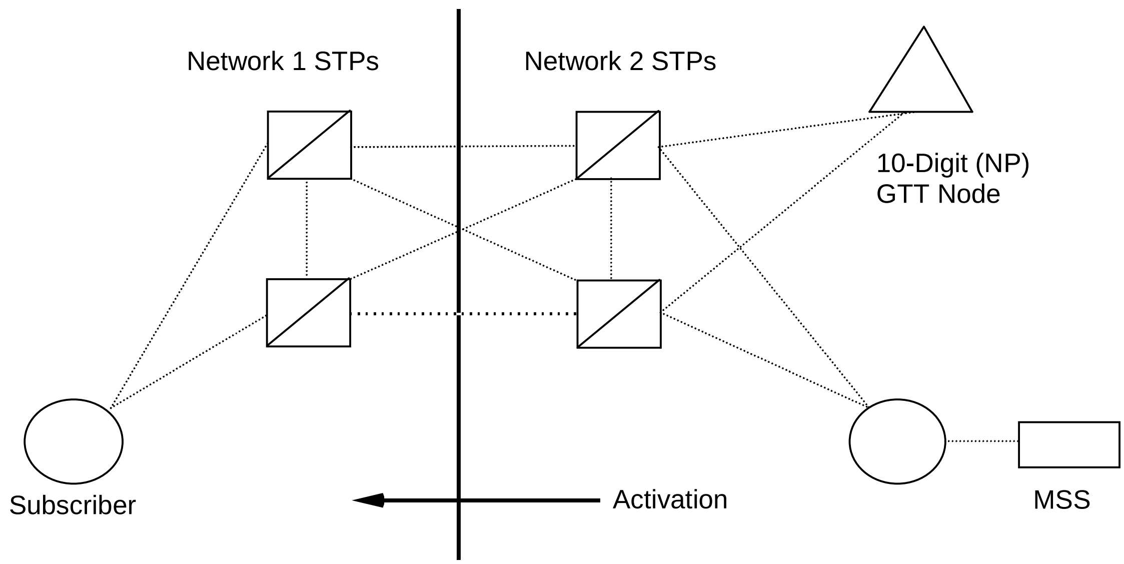


Figure B-25/ATIS-1000112.3 - NP Message Waiting Example Diagram

B.31.4 Global Title Translation Requirements

After a 10-digit GTT is performed, a translation will be performed at a subsequent GTT node. The global title address information takes one of the following two forms:

1. When the subsequent GTT node supports translation of ported numbers for this translation type, the address information is the ten digit called (subscriber) number.
2. [optionally by network] When the subsequent GTT node does not support translation of ported numbers for this translation type, the address information is either:
    a. The ten digit called (subscriber) number when that number is not ported.
    b. A routing number, supplied by the 10-digit (NP) GTT function, when the called (subscriber) number is ported.

This information is encoded as BCD. Global Title Indicator type 2 will be used. Either the first 3, 6, or 10 digits of the global title address information will be sufficient to perform the final GTT. The output of the final GTT will be the point code of the SEP serving the subscriber's called party number and the SSN of the application.

B.31.5 Relationship to Existing Application/Translation Groups

This application is very similar to the Message Waiting application group, but translation requirements are different due to the impacts of Number Portability on the routing of Message Waiting queries. This application/translation group provides a mechanism to prevent looping.

Annex C
(informative)

ANNEX C MAPPING FOR CAUSE PARAMETER VALUES

C.1 Introduction

During connection refusal/release/reset, the SCCP and its users could take necessary corrective actions, if any, only upon relevant information available to them. Thus, it would be very helpful if that information could be conveyed correctly.

During connection release, the "release cause" parameter in the *Released* (RLSD) message and the N-DISCONNECT primitive (with parameters "originator" and "reason") are used together to convey those information on the initiator and the cause of the connection release. In addition, the N-DISCONNECT primitive is also used together with the "refusal cause" parameter in the *Connection Refused* (CREF) message to convey that information during connection refusal. During connection reset, the "reset cause" parameter in the Reset *Request* (RSR) message and the N-RESET primitive (with parameters "originator" and "reason") are used together similarly.

In order to convey those information correctly, this Annex provides a guideline for the mapping of values between the cause parameters and the corresponding N-primitive parameters during various scenarios.

C.2 Connection Refusal

Table C-1/ATIS-1000112.3 describes the mapping of values between the "refusal cause" parameter (clause 3.15 of ATIS-1000112.3) and the "originator", "reason" parameters in the N-DISCONNECT primitive (clause 2.1.1.2.4 of ATIS-1000112.1).

Table C-1/ATIS-1000112.3 - Mapping During Connection Refusal

CREF Message		N-DISCONNECT Primitive	
Code	Refusal Cause	Reason	Originator*
00000000	end user originated	conn. refusal - end user originated	NSU
00000001	end user congestion	conn. refusal - end user congestion	NSU
00000010	end user failure	conn. refusal - end user failure	NSU
00000011	SCCP user originated	conn. refusal - SCCP user originated	NSU
00000100	destination address unknown	conn. refusal - destination address unknown (non-transient cond.)	NSP
00000101	destination inaccessible	conn. refusal - destination inaccessible/transient cond.	NSP
00000110	network resource - QoS unavailable/non-transient	conn. refusal - QoS unavailable/ non-transient condition	NSP[1]
00000111	network resource - QoS unavailable/transient	conn. refusal - QoS unavailable/ transient condition	NSP[1]
00001000	access failure	conn. refusal - access failure	NSU
00001001	access congestion	conn. refusal - access congestion	NSU
00001010	subsystem failure	conn. refusal - subsystem failure	NSP
00001011	subsystem congestion[2]	conn. refusal - subsystem congestion	NSU
00001100	expiration of connection est. timer	conn. refusal - reason unspecified/transient	NSP[1]
00001101	incomplete user data	conn. refusal - incompatible info in NSDU	NSU
00001110	not obtainable	conn. refusal - reason unspecified/transient	NSP[1]
00001110	not obtainable	conn. refusal - undefined	undefined
00001111	unqualified	conn. refusal - reason unspecified/transient	NSP[1]
00001111	unqualified	conn. refusal - undefined	undefined
00010000	hop counter violation	conn. refusal – hop counter violation	NSP
00010010	no translation of such nature	conn. refusal – destination address unknown/non-transient condition	NSP
00010011	unequipped user	conn. refusal – destination inaccessible/non-transient condition	NSP

* NSU - Network Service User; NSP - Network Service Provider.

[1] Only those cases will be applicable if SCCP originates the refusal procedure in response to REQUEST interface element.

[2] Procedures associated with subsystem congestion are for further study.

C.3 Connection Release.

Table C-2/ATIS-1000112.3 describes the mapping of values between the "release cause" parameter (clause 3.11 of ATIS-1000112.3) and the "originator," "reason" parameters in the N-DISCONNECT primitive (clause 2.1.1.2.4 of ATIS-1000112.1).

Table C-2/ATIS-1000112.3 - Mapping During Connection Refusal

RLSD Message		N-DISCONNECT Primitive	
Code	Release Cause	Reason	Originator*
00000000	end user originated	disconnection - normal condition	NSU
00000001	end user congestion	disconnection - end user congestion	NSU
00000010	end user failure	disconnection - end user failure	NSU
00000011	SCCP user originated	disconnection - SCCP user originated	NSU
00000100	remote procedure error	disconnection - abnormal condition of transient nature	NSP
00000101	inconsistent connection data	disconnection - abnormal condition of transient nature	NSP
00000110	access failure	disconnection - access failure	NSU
00000111	access congestion	disconnection - access congestion	NSU
00001000	subsystem failure	disconnection - subsystem failure	NSP
00001001	subsystem congestion[1]	disconnection - subsystem congestion	NSU
00001010	network failure	disconnection - network failure	NSP
00001011	network congestion	disconnection - network congestion	NSP
00001100	expiration of reset timer	disconnection - abnormal condition of transient nature	NSP
00001101	expiration of receive inactivity timer	disconnection - abnormal condition of transient nature	NSP
00001110	not obtainable	disconnection - undefined	NSP
00001110	not obtainable	disconnection - undefined	undefined
00001111	unqualified	disconnection - abnormal condition	NSU
00001111	unqualified	disconnection - undefined	NSP
00001111	unqualified	disconnection - undefined	undefined
* NSU - Network Service User; NSP - Network Service Provider. [1] Procedures associated with subsystem congestion are for further study.			

C.4 Connection Reset

Table C-3/ATIS-1000112.3 describes the mapping of values between the "reset cause" parameter (clause 3.13 of ATIS-1000112.3) and the "originator", "reason" parameters in the N-RESET primitive (clause 2.1.1.2.3 of ATIS-1000112.1).

Table C-3/ATIS-1000112.3 - Mapping During Connection Reset

RSR Message		N-RESET Primitive	
Code	Reset Cause	Reason	Originator*
00000000	end user originated	reset - user synchronization	NSU
00000001	SCCP user originated	reset - user synchronization	NSU
00000010	message out of order - incorrect P(S)	reset - unspecified	NSP
00000011	message out of order - incorrect P(R)	reset - unspecified	NSP
00000100	remote procedure error - message out of window	reset - unspecified	NSP
00000101	remote procedure error - incorrect P(S) after initialization	reset - unspecified	NSP
00000110	remote procedure error - general	reset - unspecified	NSP
00000111	remote end user operational	reset - user synchronization	NSU
00001000	network operational	reset - unspecified	NSP
00001001	access operational	reset - user synchronization	NSU
00001010	network congestion	reset - network congestion	NSP
00001011	not obtainable	reset - unspecified	NSP
00001011	not obtainable	reset - undefined	undefined
00001100	unqualified	reset - unspecified	NSP
00001100	unqualified	reset - undefined	undefined
* NSU - Network Service User; NSP - Network Service Provider.			

ATIS-1000112.4.2005

[Revision of T1.112.4-2001]

Chapter 4
Signaling Connection Control Part Procedures (SCCP)

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

American National Standard for Telecommunications –

Signaling Connection Control Part Procedures (SCCP)

1 Scope, Purpose, and Application

1.1 General Characteristics of Signaling Connection Control Procedures

This chapter may contain requirements that reference other American National Standards. If so, when the American National Standards referenced in the requirements are superseded by revisions approved by ANSI, the revisions shall apply.

1.1.1 Purpose

This chapter describes the procedures performed by the Signaling Connection Control Part (SCCP) of Signaling System No. 7 (SS7) to provide both connection-oriented and connectionless network services, and SCCP management services as defined in ATIS-1000112.1. These procedures make use of the messages and information elements defined in ATIS-1000112.2, whose formatting and coding aspects are specified in ATIS-1000112.3.

1.1.2 Protocol Classes

The protocol used by the SCCP to provide network services is subdivided into four protocol classes, defined as follows:

1. *Class 0*: Basic connectionless class;
2. *Class 1*: Sequenced (MTP) connectionless class;
3. *Class 2*: Basic connection-oriented class; and
4. *Class 3*: Flow control connection-oriented class.

The connectionless protocol classes provide those capabilities that are necessary to transfer one Network Service Data Unit (NSDU) (i.e., one user-to-user information block) in the user data field of a *UDT/XUDT/LUDT* or *UDTS/XUDTS/LUDTS* message.

When one connectionless message is not sufficient to convey the user data contained in one NSDU making use of the MTP services provided by an MTP network that supports a maximum MTP SDU size of 272 octets including the MTP routing label, a segmenting/reassembly function of protocol class 0 and 1 is provided. In this case, the SCCP at the originating node or in a relay node provides segmentation of the information into multiple segments prior to transfer in the "data" field of *XUDT* (or as a network option *LUDT*) messages. At the destination node, the NSDU is reassembled.

If it is certain that only MTP services supporting a maximum MTP-SDU size of 4095 octets are used in the network, then no segmentation information is needed.

The connection-oriented protocol classes (protocol classes 2 and 3) provide the means to setup signaling connections in order to exchange a number of related NSDUs. The connection-oriented protocol classes also provide a segmenting and reassembly capabilities. If a Network Service Data Unit is longer than 255[1] octets, it is split into multiple segments at the originating node, prior to transfer in the "data" field of *Data* messages. Each segment is less than or equal to 255[1] octets. At the destination node, the NSDU is reassembled.

NOTE - Enhancements to protocol class 2 and 3 for the SCCP capable of supporting long messages are for further study.

1.1.2.1 Protocol Class 0

Network Service Data Units passed by higher layers to the SCCP in the node of origin are delivered by the SCCP to higher layers in the destination node. They are transported independently of each other. Therefore, they may be delivered out-of-sequence. Thus, this protocol class corresponds to a pure connectionless network service.

1.1.2.2 Protocol Class 1

In protocol class 1, the features of class 0 are complemented by an additional feature (i.e., sequence control parameter associated with the N-UNITDATA request primitive) which allows the higher layer to indicate to the SCCP that a given stream of NSDUs have to be delivered in-sequence. The Signaling Link Selection (SLS) field is chosen, based on the value of the sequence control parameter. The SLS chosen for a stream of NSDUs with the same sequence control parameter will be identical. The SCCP will then encode the SLS field in the routing label of messages relating to such NSDUs, so that their sequence is, under normal conditions, maintained by the signaling network as defined in ATIS-1000111.4. Thus, this class corresponds to an enhanced connectionless service, where an additional sequencing feature is included.

If a *UDT/XUDT/LUDT* message is received at an intermediate SCCP node, and the protocol class is set to 1, then the SCCP should ensure that an incoming sequence of messages with the same SLS code from the same origin is preserved on the outgoing link. If a translation is being performed at the node and *UDT/XUDT/LUDT* message is received with protocol class 1, then during normal operation, the translation should yield identical results for any message with the same address information of such a message sequence.

1.1.2.3 Protocol Class 2

In protocol class 2, bi-directional transfer of NSDUs between the user of the SCCP in the node of origin and the user of the SCCP in the destination node is performed by setting up a temporary or permanent

---

[1] The transfer of up to 254 or 255 octets of user data is allowed, provided that the maximum length of the signaling information field (SIF) as specified in 2.3.8 of ATIS-1000.111.3 is not exceeded.

signaling connection. A number of signaling connections may be multiplexed onto the same signaling relation, as defined in ATIS-1000111.4; such a multiplexing is performed by using a pair of reference numbers, referred to as *local reference numbers*. Messages belonging to a given signaling connection will contain the same value of the SLS field to ensure sequencing as described in clause 1.1.2.2. Thus, this protocol class corresponds to a simple connection-oriented network service, where SCCP flow control and message sequencing are not provided.

The quality of service -- in terms of message loss, undetected errors, mis-sequencing, etc. -- is the same as that offered by the Message Transfer Part (MTP) to the User Parts.

1.1.2.4 Protocol Class 3

In protocol class 3, the features of protocol class 2 are complemented by the inclusion of flow control, with its associated capability of expedited data transfer. Moreover, an additional capability of detection of message loss or mis-sequencing is included for each connection section; in such a circumstance, the signaling connection is reset and a corresponding notification is given by the SCCP to the higher layers.

1.1.3 Signaling Connections

In all connection-oriented protocol classes, a signaling connection between the nodes of origin and destination may consist of:

- A single connection section; or
- A number of connection sections in tandem, which may belong to different interconnected signaling networks.

In the former case, the originating and destination nodes of the signaling connection coincide with the originating and destination nodes of a connection section. During the connection establishment phase, SCCP routing and relaying functions, as described in clause 2 of this Chapter, may be required at one or more intermediate nodes. Once this signaling connection has been established, though, SCCP functions are not required at intermediate nodes.

In the latter case, at any intermediate node where a message is received from a connection section and has to be sent on another connection section, the SCCP routing and relaying functions are involved during connection establishment. In addition, SCCP functions are required at intermediate nodes during data transfer and connection release to provide association of connection sections.

1.1.4 Compatibility and Handling of Unrecognized Information

1.1.4.1 Rules For Forward Compatibility

All implementations must recognize all messages in each protocol class offered, as indicated in Table 1/ATIS-1000112.3. Further study is required on the reaction to messages of an unsupported class (e.g., class 3 messages when only class 0 and 1 are supported).

1.1.4.2 Handling of Unrecognized Messages or Parameters

Any message with an unrecognized type value shall be discarded.

Any unrecognized parameter within a message shall be ignored and passed on transparently.

1.1.4.3 Handling of Unsupported Optional Parameter Value

When an unsupported optional parameter value is detected by the SCCP, then the parameter value shall be passed on transparently.

1.1.4.4 Treatment of Spare Fields

The SCCP shall handle spare fields in SCCP messages in the following manner:

- Spare fields or subfields are set to zero on message creation;
- Spare fields or subfields are not examined at intermediate nodes nor at the destination nodes; and
- Spare fields or subfields shall remain unchanged in relay nodes.

1.1.4.5 Handling of Gaps

Gaps (refer to ATIS-1000113.3, clause 1.5) can exist without causing errors, but they are not desirable. Whether or not gaps can occur in existing implementations is implementation dependent, but implementation of this version of the SCCP shall not introduce any gaps. For compatibility reasons, the SCCP shall not make specific checks for gaps; but if any gaps are detected, the message shall be processed as though the gaps were not present. The gaps are considered not to be part of the message and may be deleted when reformatting the message. Although no gaps are allowed to be sent (refer to ATIS-1000112.3, clause 1.5), a received gap is allowed and has to be ignored.

1.2 Overview of Procedures for Connection-Oriented Services

1.2.1 Connection Establishment

When the SCCP functions at the node of origin receive a request to establish a signaling connection, the Called Party Address is analyzed to identify the node towards which the signaling connection should be established. If the node is not the same, the SCCP forwards a *Connection Request* (CR) message to that signaling point, using the MTP functions.

The SCCP in the node receiving the *CR* message via the MTP functions examines the Called Party Address, and one of the following actions takes place at the node:

1. If the Called Party Address contained in the *CR* message corresponds to a user located in that signaling point, and if the signaling connection may be established (i.e., establishment of a signaling connection is agreed to by the SCCP and local user), a *Connection Confirm* (CC) message is returned.

2. If the Called Party Address is not that signaling point, then information available in the message and at the node are examined to determine whether an association of two connection sections is required at that node.

    - If an association is required, then the SCCP establishes an (incoming) signaling connection section. Establishment of another (outgoing) connection section is initiated by sending a *CR* message towards the next node, and this connection section is logically linked to the incoming connection section.

    - If coupling of the connection section is not required in this node, no incoming or outgoing connection section is established. A *CR* message is forwarded towards the next destination using the MTP routing function.

If the SCCP receives a *CR* message and either the SCCP or the SCCP user does not wish to establish the connection, then a *Connection Refused* (CREF) message is transferred on the incoming connection section.

On receipt of a *CC* message, the SCCP completes the set-up of a connection section. Furthermore, if coupling of two adjacent connection sections is needed, a further *CC* message is forwarded to the preceding node.

If no coupling of adjacent connection sections was needed during set-up in the forward direction, the *CC* message can be sent directly to the node of origin, even if a number of intermediate SCCP nodes were passed in the forward direction. The OPC of the node of origin is transmitted within the Calling Party Address field.

When the *CR* and *CC* messages have been exchanged between all the involved nodes as above described, and the corresponding indications have been given to a higher layer functions in the nodes of origin and destination, then the signaling connection is established and transmission of messages may commence.

1.2.2 Data Transfer

Transfer of each NSDU is performed by one or more *Data Form 1/2* (*DT*) messages; a more-data indication is used if the NSDU is to be split among more than one *DT* message. If protocol class 3 is used, then SCCP flow control is exploited over each connection section of the signaling connection. If, in such protocol classes, abnormal conditions are detected, then the appropriate actions are taken on the signaling connection (e.g., reset). Moreover, in such protocol classes, expedited data may be sent using one *Expedited Data (ED)* message that bypasses the flow control procedures applying to *DT* messages. A limited amount of data may also be transferred in the *CR*, *CC, CREF*, and *RLSD* messages.

1.2.3 Connection Release

When the signaling connection is terminated, a release sequence takes place on all connection sections by means of two messages called *Released* (*RLSD*) and *Release Complete* (*RLC*). Normally, in reaction to the receipt of *RLSD* message the *RLC* message is sent.

1.3 Overview of Procedures for Connectionless Services

1.3.1 General

When the SCCP functions at the node of origin receive from a higher layer the user data to be transferred by the protocol class 0 or 1 connectionless service, the Called Address and other relevant parameters, if required, are analyzed to identify the node towards which the message should be sent. The user data is then included as user data in a *UDT/XUDT/LUDT* message, which is sent towards the node using the MTP functions. If the network structure is such that both *LUDT(S)* and *XUDT(S)* messages may apply, then routing may transmit a message other than *LUDT(S)* (see clause 2.5). Upon receipt of the *UDT/XUDT/LUDT* message, the SCCP functions at that node perform the routing analysis as described in clause 2 of this chapter and -- if the destination of the *UDT/XUDT/LUDT* message is a local user -- deliver the user data to the local higher layer functions. If the Called Party Address is not at that node, then the *UDT/XUDT/LUDT* message is forwarded to the next node after a possible change of the type of message (see clause 2.5). This process continues until the NSDU has reached the Called Party Address.

1.4 Structure of the SCCP and Contents of Specification

The basic structure of the SCCP appears in Figure 1/ATIS-1000112.4. It consists of four functional blocks:

1. *SCCP connection-oriented control:* Its purpose is to control the establishment and release of signaling connections, and to provide for data transfer on signaling connections.
2. *SCCP connectionless control:* Its purpose is to provide for the connectionless transfer of data units.
3. *SCCP management:* Its purpose is to provide capabilities, in addition to the Signaling Route Management and flow control functions of the MTP, to handle the congestion or failure of either the SCCP user or the signaling route to the SCCP user.
4. *SCCP routing:* Upon receipt of a message from the MTP or from functions 1 or 2 above, SCCP routing provides the necessary routing functions to either forward the message to the MTP for transfer, or pass the message to functions 1 or 2 above. A message whose Called Party Address is a local user is passed to functions 1 or 2, while one destined for a remote user is forwarded to the MTP for transfer to a distant SCCP user unless a compatibility test occurs which result in passing the message to function 2.

Clause 2 of this specification describes the addressing and routing functions performed by the SCCP. Clause 3 specifies the procedures for the connection-oriented services (protocol classes 2-3). Clause 4 specifies the procedures for the connectionless services (protocol classes 0 and 1). Clause 5 specifies the SCCP management procedures. Clause 6 consists of the state transition diagrams that correspond to the text.

2 ADDRESSING AND ROUTING

2.1 SCCP Addressing

The Called and Calling Party Addresses contain the information necessary for the SCCP to determine an origination and destination node. In the case of the connection-oriented procedures, the addresses are the origination and destination points of the signaling connection, while in the case of the connectionless procedures, the addresses are the origination and destination points of the message.

When transferring connection-oriented or connectionless messages, two basic categories of addresses are distinguished by SCCP routing:

1. *Global Title* - A global title is an address -- such as dialed-digits -- that does not explicitly contain information that would allow routing in the signaling network. The translation function of the SCCP is required.
2. *PC + SSN* - A Point Code and Subsystem Number allow direct routing by the SCCP and MTP; that is, the translation function of the SCCP is not required. The point code from the called address is used as the DPC in the routing label. In the calling address, the point code is either supplied by the Calling Party Address parameter, or if not present, by the OPC in the routing label.

Global title addressing may be used when the SCCP translation function is required for routing. The global title information may be supplemented by optional routing parameter information, for example ISNI parameter. See clause 2.2.2.2. This translation function could be performed on a distributed basis or on a centralized basis. The last case, where a request for translation is sent to a centralized database while waiting for the response, is for further study.

If a reply or a message return is required, the Calling Party Address plus the OPC in the routing label must contain sufficient information to uniquely identify the originator of the message. If the message requires global title translation where the OPC may change, then the Calling Party Address should not contain an SSN only.

2.2 SCCP Routing Principles

SCCP routing control (SCRC) receives messages from the MTP for routing and discrimination, after they have been received by the MTP from another node in the signaling network. SCRC also receives internal messages from SCCP connection-oriented control (SCOC) and connectionless control (SCLC) and performs any necessary routing functions (e.g., address translation) before passing them to the MTP for transport in the signaling network or back to the SCCP connection-oriented or connectionless control.

The routing function consists of:

1. Determining an SCCP node towards which the message is allowed to be sent;
2. Performing the compatibility test.

SCRC may also translate (e.g., for security reasons) a Calling Party Address from PC + SSN to GT. This function is optional depending on the security requirements of network interconnections.

2.2.1 Receipt of SCCP Message Transferred by the MTP

A message transferred by the MTP that requires routing will include the Called Party Address parameter (and any optional routing parameter) giving information for routing the message. These messages currently include the *CR* message and all types of connectionless messages. All connection oriented messages except the *CR* message are passed directly to SCOC.

NOTE – The called party address in the *CREF* or *CC* messages shall not be used for routing.

If the Called Party Address parameter is used for routing, the routing indicator indicates whether the routing is based on:

1. *Subsystem Number only* - This indicates that the receiving SCCP is the termination point of the message. The SSN is used to determine the local subsystem.
2. *Global Title (and any optional routing parameter) only* - This indicates that translation is required. Translation of the Global Title (and any optional routing parameter) results in a new DPC for routing the message, and possibly a new SSN or GT and a new address indicator.

If the SPC is present in the Called Party Address, it is not used by SCRC.

2.2.2 Messages from Connection-Oriented or Connectionless Control to SCCP Routing Control

Addressing information, indicating the destination of the message, is included with every internal message received from connection-oriented or connectionless control. For connectionless messages, this addressing information is obtained from the Called Address parameter associated with the N-UNITDATA request primitive.

For *CR* messages received by SCCP routing, the addressing information is obtained from the Called Address parameter associated with the N-CONNECT request primitive or from the addressing information contained in the received *CR* message and made available to SCOC (the latter case refers to intermediate node with association of connections). For connection-oriented messages other than a *CR* message, the addressing information (i.e., the DPC) is that associated with the connection section over which the message is to be sent. The addressing information can take the following forms:

1. DPC;
2. DPC + (SSN or GT or both);
3. GT; or
4. GT + SSN.

The first form applies to connection-oriented messages except the *CR* message. The last three forms apply to connectionless messages and to the *CR* message.

2.2.2.1 DPC Present

If the DPC is present in the addressing information, and the DPC is not the node itself, then the DPC is passed to the MTP using the MTP-TRANSFER request primitive and:

1. If no other addressing information is available (case 1 of 2.2.2), no Called Party Address is provided in the message.
2. For case 2 of clause 2.2.2:
    a. If the message is a *CR* message and the association of the connection section is indicated (i.e., intermediate node), then the message is passed to the MTP with the same addressing information made available to SCOC as before the association of connection sections.
    b. If the message is a connectionless message or a *CR* message at the node where the message originates then the DPC is used as the destination point code in the MTP-TRANSFER request primitive.

If the DPC is the node itself (case 2 of clause 2.2.2), then the message is passed based on the message type to either connection-oriented control or connectionless control based on the availability of the specified internal subsystem.

2.2.2.2 Translation Required

If the DPC is not present, and the routing indicator indicates route on global title (case 3 and 4 of clause 2.2.2), then a global title translation is required before the message can be sent out. Translation results in a DPC and possibly an SSN or new GT and possibly a new address indicator. The translation function will also indicate whether the routing at the destination will be based on GT or SSN. The routing procedures then continue as per clause 2.2.2.1 of ATIS-1000112.4.

2.3 SCCP Routing

The SCCP routing functions are based on information contained in the Called Party Address (and any optional routing parameter).

2.3.1 Receipt of SCCP Message Transferred by the MTP

One of the following actions is taken by SCCP routing upon receipt of a message from the MTP. The message is received by the SCCP when the MTP invokes an MTP-TRANSFER indication:

1. If the message is a connection-oriented message other than a *CR* message, then SCCP routing passes the message to connection-oriented control.
2. If the routing indicator in the Called Party Address does not indicate route on global title, then SCCP routing checks the status of the subsystem[2]:
    a. If the subsystem is available, the message is passed, based on the message type, to either connection-oriented control or connectionless control.
    b. If the subsystem is unavailable and:

[2] SCCP routing control may optionally not check the status of subsystems (e.g., SSN=1 and SSN=4) before routing to these subsystems, and therefore should consider these subsystems available.

- ♦ The message is a connectionless message, then the message return procedure is initiated;
- ♦ The message is a connection-oriented message, then the connection refusal procedure is initiated.

In addition, if the subsystem is failed, SCCP management is notified that a message was received for a failed subsystem.

3. If it is a *CR* message or a connectionless message and the routing indicator in the Called Party Address indicates route on GT, a translation of the GT (and any optional routing parameter) must be performed. The translation function will decrement the SCCP hop counter (if present) and if a hop counter violation is encountered, the appropriate routing failure procedure will be initiated.

   a. If the translation does not exist, and:

      - ♦ The message is a connectionless message, then the message return procedure is initiated.
      - ♦ The message is a connection-oriented message, then the connection refusal procedure is initiated.

   b. If the translation of the global title is successful, and both the DPC and SSN are determined, then:

      i. If the DPC is the node itself, then the procedures in (2) above are followed.

      ii. If the DPC is not the node itself, the DPC and SSN are available[3], and the message is a connectionless message, then the MTP-TRANSFER request primitive is invoked unless the compatibility test sends the message to SCLC.

      iii. If the DPC is not the node itself, the DPC and SSN are available, and the message is a *CR* message, then:

         - ♦ If an association of connection sections is required, the message is passed to connection-oriented control.
         - ♦ If no association of connection sections is required, the MTP-TRANSFER request primitive is invoked.

      iv. If the DPC is not the node itself, and the DPC and/or SSN are not available and

         - ♦ The message is a connectionless message, then the message return procedure is initiated;
         - ♦ The message is a connection-oriented message, then the connection refusal procedure is initiated.

   c. If the translation of the GT is successful and only a DPC or DPC + new GT is determined, then:

---

[3] In clauses 2.3.1 and 2.3.2 of ATIS-1000.112.4, "the DPC is available" means that the DPC is available and the message's priority is greater than or equal to the DPC's congestion level. Also, "the DPC is not available" means that the DPC is not available or the message's priority is less than the DPC's congestion level.

i. If the DPC is available, and the message is a connectionless message, then the MTP-TRANSFER request primitive is invoked unless the compatibility test sends the message to SCLC.

ii. If the DPC is available, and the message is a *CR* message, then:

- ♦ If an association of the connection sections is required, then the message is passed to connection-oriented control.
- ♦ If no association of connection sections is required, then the MTP-TRANSFER request primitive is invoked.

iii. If the DPC is not available and:

- ♦ The message is a connectionless message, then the message return procedure is initiated.
- ♦ The message is a connection-oriented message, then the connection refusal procedure is initiated.

2.3.2 Messages from Connectionless or Connection-Oriented Control to SCCP Routing Control

One of the following actions is taken by SCCP routing upon receipt of a message from connectionless control or connection-oriented control.

1. If the message is a *CR* message at an intermediate node (where connection sections are being associated), and:
   a. The DPC is available[3], then the MTP-TRANSFER request primitive is invoked.
   b. The DPC is not available[3], then the connection refusal procedure is initiated via SCOC.
2. If the message is a connection-oriented message other than a *CR* message, and:
   a. The DPC is available, then the MTP-TRANSFER request primitive is invoked.
   b. The DPC is not available, then the connection release procedure is initiated.
3. If the "Called address" primitive associated with a *CR* or connectionless message includes a DPC and the routing indicator does not indicate route on global title (i.e., route on SSN), and:
   a. The DPC and SSN are available, then the MTP-TRANSFER request primitive is invoked unless the compatibility test sends the message to SCLC.
   b. The DPC and/or SSN are not available, then:
      - ♦ For connectionless messages, the message return procedure is initiated.
      - ♦ For connection-oriented messages, the connection refusal procedure is initiated.
   c. The DPC is the node itself, then the procedures in clause 2.3.1 (2) of ATIS-1000112.4 are followed.
4. If the "Called address" primitive associated with a *CR* or connectionless message includes a DPC and the routing indicator does indicate route on global title, and:
   a. The DPC is available, then the MTP-TRANSFER request primitive is invoked unless the compatibility test sends the message to SCLC.

b. The DPC is not available then:

- ♦ For connectionless messages, the message return procedure is initiated.
- ♦ For connection-oriented messages, the connection refusal procedure is initiated.

c. The DPC is the node itself, then the procedures in clause 2.3.2 (5) of ATIS-1000112.4 are followed.

5. If the "Called address" primitive associated with a *CR* or connectionless message does not include a DPC and the routing indicator does indicate route on global title, then a translation of the global title must be performed.

a. If the translation of the global title (and any optional routing parameter) does not exist, and:

- ♦ The message is a connectionless message, then the message return procedure is initiated.
- ♦ The message is a connection-oriented message, then the connection refusal procedure is initiated.

b. If the translation of the global title (and any optional routing parameter) exists, and both the DPC and SSN are determined, then:

i. If the DPC is the node itself, then the procedures in clause 2.3.1 (2) of ATIS-1000112.4 are followed[4].

ii. If the DPC is not the node itself and DPC and SSN are available, then the MTP-TRANSFER request primitive is invoked unless the compatibility test sends the message to SCLC[5].

iii. If the DPC is not the node itself, and the DPC and/or SSN are not available and:

- ♦ The message is a connectionless message, then the message return procedure is initiated.
- ♦ The message is a connection-oriented message, then the connection refusal procedure is initiated.

c. If the translation of the global title exists and only a DPC or DPC + new GT is determined, then:

i. If the DPC is available, then the MTP-TRANSFER request primitive is invoked *unless the compatibility test sends the message to SCLC*.

ii. If the DPC is not available and:

- ♦ The message is a connectionless message, then the message return procedure is initiated.

---

[4] The function of routing between local subsystems is implementation dependent.

[5] This clause combines 2.3.2 (4) (ii) and 2.3.2 (4) (iii) of the CCITT Red Book, Volume VI, which distinguished connectionless and connection-oriented messages but resulted in the same procedure being followed once the need for association of connection sections at this point was deleted.

♦ The message is a connection-oriented message, then the connection refusal procedure is initiated.

6. Other actions are not specified for the U.S.[6]

NOTE - In this section, if SCCP routing cannot determine the status of a Point Code or Subsystem, SCCP considers the status as "available."

2.4 Routing Failures

The SCCP recognizes a number of reasons for failure in SCCP routing control. Some examples of these reasons are:

1. Translation does not exist for addresses of this nature;
2. Translation does not exist for this specific address;
3. Network/subsystem failure;
4. Network/subsystem congestion;
5. Unequipped user; and
6. Hop Counter Violation.

The precise classification of the causes by which such failures are recognized is for further study.

When SCCP routing is unable to transfer a message due to the unavailability of a Point Code or Subsystem, one of the above reasons is indicated in the *CREF message, or the UDTS/XUDTS/LUDTS* message.

2.5 Compatibility test

The compatibility test defined in this clause applies to connectionless procedures only.

If the network structure is such that incompatibilities requiring segmentation, truncation, or message type change are never present, then the compatibility test is not required.

Based on the available knowledge at the local node[7], the compatibility test ensures that:

1. The SCRC never attempts to send a message that cannot be understood by the recipient SCCP node.
2. The outgoing messages are of the appropriate length to be carried by the underlying MTP.

The compatibility test in SCRC determines whether:

1. An *LUDT* message needs to be segmented.

---

[6] An additional procedure was deleted from the March 1985 CCITT text.

[7] NOTE - The information to be provisioned about the adjacent SCCP nodes' message handling capability (e.g., *UDT*, *XUDT*) would depend on network configurations. Also, depending on network configurations, it may be possible to provision the message handling capability of an entire interconnecting network as a single entity, as opposed to each individual node in the interconnecting network.

2. An *LUDTS* message needs to be truncated.
3. The message type needs to be changed. In some cases, a message may be changed to a type preferred by the recipient node (clause 4.1.2).

If no segmentation, truncation, or message type change is required, then the MTP-TRANSFER primitive is invoked. Otherwise, the message is passed to SCLC for the necessary changes.

3 CONNECTION-ORIENTED PROCEDURES

3.1 Connection Establishment

3.1.1 General

The connection establishment procedures consist of the functions required to establish a temporary signaling connection between two users of the SCCP.

The connection establishment procedures are initiated by an SCCP user by invoking the N-CONNECT request primitive.

The ISUP may initiate an SCCP connection in the same way as any other user, but may also request the SCCP to initiate a connection and return the information to the ISUP for transmission in an ISUP message.

The signaling connections between two users of the SCCP, which are referred to by the "Called/Calling address" parameters in the N-CONNECT request primitive, may be realized by the establishment of one or more connection sections. The SCCP user is not aware of how the SCCP provides the signaling connection (e.g., by one or more than one connection sections).

The realization of a signaling connection between two SCCP users then can be described by the following components:

1. One or more connection sections;
2. An originating node, where the "Calling address" is located;
3. Zero or more relay nodes with coupling, where, for this signaling connection, there is no distribution to an SCCP user; and;
4. A destination node, where the "Called address" is located.

The *CR* message and the *CC* message are used to setup connection sections.

3.1.2 Local Reference Numbers

During connection establishment, both a source and destination local reference number are assigned independently to a connection section.

Source and destination local reference numbers are assigned at connection section setup for a permanent connection section.

Once the destination reference number is known, it is a mandatory field for all messages transferred on that connection section.

Each node will select the local reference that will be used by the remote node as the destination local reference number field on a connection section for data transfer.

The local reference numbers remain unavailable for use on other connection sections until the connection section is released and the reference numbers are removed from their frozen state. See also clause 3.3.2.

3.1.3 Negotiation Procedures

3.1.3.1 Protocol Class Negotiation

During connection establishment, it is possible to negotiate the protocol class of a signaling connection between two SCCP users.

The N-CONNECT request primitive contains a parameter, the "Quality of service parameter set," with the preferred quality of service proposed by the SCCP user for the signaling connection.

The SCCP at the originating, relay, and destination nodes may alter the protocol class on a signaling connection so that the QoS assigned to the signaling connection is less restrictive (e.g., a protocol class 2 connection may be provided if a protocol class 3 connection is proposed). Information concerning the present proposed protocol class within the SCCP is carried in the *CR* message, and the assigned protocol class appears in the *CC* message.

At the destination node, the SCCP user is notified of the proposed class using the N-CONNECT indication primitive.

The protocol class of a signaling connection may also be altered by the Called SCCP user in the same manner (i.e., less restrictive) when invoking the N-CONNECT response primitive.

The Calling SCCP user is informed of the QoS selected on the signaling connection using the N-CONNECT confirmation primitive.

3.1.3.2 Flow Control Credit Negotiation

During connection establishment, it is possible to negotiate the window size to be used on a signaling connection for the purpose of flow control. This window size remains fixed for the life of the signaling connection. The credit field in the *CR* and *CC* messages is used to indicate the maximum window size.

The N-CONNECT request primitive contains a parameter, the "Quality of service parameter set" with the preferred quality of service proposed by the SCCP user for the signaling connection.

The SCCP at the originating, relay, and destination nodes may alter the window size on a signaling connection so that the quality of service assigned to the signaling connection is less restrictive (e.g., a smaller window size may be provided). Information concerning the present proposed window size within the SCCP is carried in the *CR* message and the assigned maximum window size appears in the credit field of the *CC* message.

At the destination node the SCCP user is notified of the proposed window size using the N-CONNECT indication primitive.

The window size of a signaling connection may also be altered by the Called SCCP user in the same manner (i.e., less restrictive) when invoking the N-CONNECT response primitive.

The Calling SCCP user is informed of the quality of service selected on the signaling connection using the N-CONNECT confirmation primitive.

3.1.4 Actions at the Originating Node

3.1.4.1 Initial Actions

The N-CONNECT request primitive is invoked by the SCCP user at the originating node to request the establishment of a signaling connection to the "Called address" contained in the primitive. The node determines if resources are available.

If resources are not available, then the connection refusal procedure is initiated.

If resources are available, then the following actions take place at the origination node:

1. A source local reference number and an SLS code are assigned to the connection section;
2. The proposed protocol class is determined for the connection section. If this protocol class provides for flow control, then an initial credit is determined;
3. A *CR* message is then forwarded to SCRC for transfer; and
4. A timer T(conn.est) is started.

The ISUP may request the SCCP to setup an SCCP signaling connection and return the information normally carried in a *CR* message to the ISUP for transmission in an ISUP message.

When the ISUP notifies the SCCP of the need for the connection, using the REQUEST Type 1 interface element, the SCCP determines if resources are available.

If resources are not available, then the connection refusal procedure is initiated.

If resources are available, then the following actions take place at the originating node:

1. A source local reference number and an SLS code are assigned to the connection section;
2. The proposed protocol class is determined for the connection section. If the protocol class provides for flow control, then an initial credit is determined;
3. An indication that the call request is from the ISUP is associated with the connection section;
4. The information that would normally be included in a *CR* message is passed to the ISUP for transfer using the REPLY interface element; and
5. A timer T(conn.est) is started.

3.1.4.2 Subsequent Actions

When an originating node receives a *CC* message, the following actions are performed:

1. The received local reference number is associated with the connection section;
2. The protocol class and initial credit for flow control of the connection section are updated if necessary;
3. The originating node of the *CC* message (identified by the OPC in the MTP label) is associated with the connection section;
4. The SCCP user is informed of the successful establishment of the signaling connection using the N-CONNECT confirmation primitive;
5. The timer T(conn.est) is stopped; and
6. The inactivity control timers, T(ias) and T(iar), are started.

When the SCCP user at an originating node invokes the N-DISCONNECT request primitive, no action is taken prior to receipt of a *CC* or a *CREF* message or expiration of the connection establishment timer.

When an originating node receives a *CREF* message, the connection refusal procedure is completed at the originating node (see clause 3.2.3).

When the connection establishment timer at the originating node expires, or when SCOC is informed of a routing failure, then the N-DISCONNECT indication primitive is invoked, the resources associated with the connection section are released, and the local reference number is frozen.

3.1.5 Actions at Relay Node with Coupling

3.1.5.1 Initial Actions.

When a *CR* message is received at a node and the SCCP routing and discrimination function determines that the "called party address" is not a local SCCP user and that a coupling is required at this node, the relay node determines if resources are available to establish the connection section.

If resources are not available at the node, or if SCOC is informed of a routing failure, then the connection refusal procedure is initiated.

Otherwise the following actions are performed:

1. A local reference number and an SLS code are assigned to the incoming connection section.

   NOTE - As an implementation option, a local reference number and an SLS code may be assigned later upon reception of a *CC* message.
2. The originating node of the *CR* message (identified by the OPC in the calling party address or by default by the OPC in the MTP label) is associated with the incoming connection section;
3. An outgoing connection section is initialized:
   - ♦ A local reference number and an SLS code are assigned to the outgoing connection section;
   - ♦ A protocol class is proposed;
   - ♦ If the proposed protocol class provides for flow control, then an initial credit for flow control is determined;
   - ♦ The *CR* message is forwarded to SCRC;
   - ♦ The timer T(conn.est) is started.

4. A coupling is made between the incoming and outgoing connection sections.

The ISUP informs the SCCP that a *CR* has been received using the REQUEST Type 2 interface element. The ISUP passes the information contained in the ISUP message to the SCCP, and indicates that a coupling is required at this node. The SCCP at the relay node then determines if resources are available to establish the connection section.

If resources are not available at the node, then the connection refusal procedure is initiated.

If resources are available at the node, then the following actions are performed:

1. A local reference number and an SLS code are assigned to the incoming connection section;
2. A local reference number and an SLS code are assigned to an outgoing connection section;
3. A protocol class is proposed;
4. An initial credit for flow control is assigned if appropriate;
5. A coupling is made between the incoming and outgoing connection sections;
6. The information that would normally be included in a *CR* message is passed to the ISUP for transfer in the REPLY interface element; and
7. The timer T(conn.est) is started.

3.1.5.2 Subsequent Actions

When a relay node receives a *CC* message, the following actions are performed:

1. The source local reference number in the *CC* message is associated with the outgoing connection section;
2. The protocol class and initial credit for flow control of the incoming and outgoing connection sections are updated if necessary;
3. The originating node of the *CC* message (identified by the OPC in the MTP label) is associated with the outgoing connection section;
4. The *CC* message is transferred, using the SCCP routing function, to the originating node of the associated connection section. The protocol class and credit are identical to those indicated in the received *CC* message;
5. The timer T(conn.est) is stopped; and
6. The inactivity control timers, T(ias) and T(iar), are started on both connection sections.

When a relay node receives a *CREF* message, the connection refusal procedure is completed at that node (see clause 3.2.2).

When the connection establishment timer expires at a relay node, the following actions are performed:

1. The resources associated with the connection are released;
2. The local reference number is frozen (see clause 3.3.2);
3. If the connection section was established using a REQUEST interface element, then the N-DISCONNECT indication primitive is invoked; and

4. The connection refusal procedure is initiated on the associated connection section (see clause 3.2.1).

3.1.6 Actions at the Destination Node

3.1.6.1 Initial Actions

When a *CR* message is received at a node, and the SCCP routing and discrimination function determines that the "called party address" is a local user, the destination node determines if resources are available to establish the connection section.

If resources are not available at the node or if SCOC is informed of a routing failure, then the connection refusal procedure is initiated.

If the resources are available at the node, then the following actions are performed:

1. A local reference number and an SLS code are assigned to the incoming connection section. (Note - As an implementation option, a local reference number may be assigned later upon reception of an N-CONNECT response primitive);
2. The originating node of the *CR* message (identified by the OPC in the calling party address or by default by the OPC in the MTP label), is associated with the incoming connection section;
3. A protocol class is proposed. If the proposed protocol class provides for flow control, then an initial credit for flow control is determined; and
4. The node informs the SCCP user of a request to establish a connection using the N-CONNECT indication primitive.

When the ISUP informs the SCCP that a *CR* has been received using the REQUEST Type 2 interface element, the ISUP passes the information contained in the ISUP message to the SCCP, and informs the SCCP that the information is for a local user. The SCCP at the destination node determines if resources are available to establish the connection section.

If resources are not available at the node, then the connection refusal procedure is initiated.

If resources are available at the node, then the following actions are performed:

1. The protocol class is determined for the connection section;
2. An initial credit for flow control is assigned if appropriate; and
3. The node informs the ISUP of the request to establish a connection using the N-CONNECT indication primitive.

3.1.6.2 Subsequent Actions

When an N-CONNECT response primitive is invoked by the SCCP user at a destination node, the following actions are performed:

1. The protocol class and credit are updated for the connection section if necessary;

2. A *CC* message is transferred, to the originating node of the incoming connection section. The protocol class and credit are identical to those indicated in the N-CONNECT response primitive; and
3. The inactivity control timers, T(ias) and T(iar), are started.

3.2 Connection Refusal

The purpose of the connection refusal procedure is to indicate to the Calling SCCP user that the attempt to setup a signaling connection section was unsuccessful.

3.2.1 Actions at Node Initiating Connection Refusal

The connection refusal procedure is initiated by either the SCCP user or the SCCP itself:

1. The SCCP user at the destination node:
   a. Uses the N-DISCONNECT request (originator indicates "network service user initiated") after the SCCP has invoked an N-CONNECT indication primitive. This is the case when the SCCP at the destination node has received the *CR* directly from a preceding SCCP; or
   b. Uses the refusal indicator in the REQUEST Type 2 interface element when the SCCP user has received the *CR* embedded in a user part message.
2. The SCCP initiates connection refusal[8] (originator indicates "network service provider initiated") due to:
   a. Limited resources at an originating, relay or destination node;
   b. Expiration of the connection establishment timer at an originating or relay node; or
   c. Routing failure.

3.2.1.1 Initiating Connection Refusal at the Destination Node.

At the destination node, the connection refusal procedure is initiated by either the SCCP (due to lack of resources or routing failure or the user (by means of an N-DISCONNECT REQUEST "primitive"). This connection refusal procedure results in the transfer of a *CREF* message on the connection section. The refusal cause contains the value of the originator in the primitives; if the refusal procedure has been initiated by using REQUEST Type 2 interface element, the refusal cause contains "SCCP user originated."

3.2.1.2 Initiating Connection Refusal at a Relay Node

If the connection refusal procedure is initiated at a relay node due to lack of resources or routing failure, then a *CREF* message is transferred on the incoming connection section.

---

[8] If the reason for the refusal is "destination address unknown", then the maintenance function is alerted.

If the connection refusal procedure is initiated at a relay node due to expiration of the connection establishment timer, then the connection release procedure is initiated on that connection section (see clause 3.3.4.1), and a *CREF* message is transferred on the associated connection section.

In either of the two above cases at the relay node: if the connection setup was initiated using a REQUEST interface element, then the SCCP user is informed by invoking the N-DISCONNECT indication primitive.

3.2.1.3 Initiating Connection Refusal at the Originating Node

At the originating node, the connection refusal procedure is initiated by the SCCP (due to lack of resources or routing failure), and the SCCP user is informed by invoking the N-DISCONNECT indication primitive.

3.2.2 Actions at a Relay Node Not Initiating Connection Refusal

When a *CREF* message is received on a connection section, the following actions are performed:

1. The resources associated with the connection section are released and the timer T(conn.est) is stopped[7];
2. If the connection was established using a REQUEST interface element, then the SCCP user is informed by invoking the N-DISCONNECT indication primitive;
3. A *CREF* message is transferred on the associated connection section; and
4. The resources associated with the associated connection section are released.

3.2.3 Actions at the Originating Node Not Initiating Connection Refusal

When a *CREF* message is received on a connection section, the following actions are performed:

1. The resources associated with the connection section are released and the timer T(conn.est) is stopped[7]; and
2. The SCCP user is informed by invoking the N-DISCONNECT indication primitive.

3.3 Connection Release

3.3.1 General

The connection release procedures consist of the functions required to release a temporary signaling connection between two users of the SCCP. Two messages are required to initiate and complete connection release: *RLSD* and *RLC*.

The release may be performed:

1. By either or both of the SCCP users to release an established connection; or
2. By the SCCP to release an established connection.

All failures to maintain a connection are indicated in this way.

3.3.2 Frozen Reference

The purpose of the frozen reference function is to prevent the initiation of incorrect procedures on a connection section due to receipt of a message that is associated with a previously established connection section.

When a connection section is released, the local reference number associated with the connection section is not immediately available for reuse on another connection section. A mechanism should be chosen to sufficiently reduce the probability of erroneously associating a message with a connection section. This particular mechanism is implementation dependent.

3.3.3 Actions at an End Node Initiating Connection Release

3.3.3.1 Initial Actions

When a connection release is initiated at an end node of a signaling connection, by the SCCP user invoking an N-DISCONNECT request primitive or by the SCCP itself, the following actions are performed at the initiating node:

1. A *RLSD* message is transferred on the connection section;
2. A release timer T(rel) is started;
3. If the release was initiated by the SCCP, then an N-DISCONNECT indication primitive is invoked; and
4. The inactivity control timers, T(ias) and T(iar), if still running, are stopped.

3.3.3.2 Subsequent Actions

The following actions are performed at the originating node on a connection section for which an *RLSD* message has been previously transferred:

1. When an *RLC* or *RLSD* message is received, the resources associated with the connection are released, the timer, T(rel), is stopped, and the local reference number is frozen; and
2. When the release timer expires, an *RLSD* message is transferred on the connection section. The sending of the *RLSD* message is repeated periodically.

When the T(rel) timer expires, T(int) and T(repeat rel) timers are started. An *RLSD* message is transferred on the connection section. When T(repeat rel) expires during the duration of T(int), it is restarted. An *RLSD* message is sent each time T(repeat rel) is restarted. Note that if congestion occurs, a longer value of T(repeat rel) might be applied.

When T(int) expires, stop T(repeat rel) if still running, release connection resources, and freeze the local reference number.

3.3.4 Actions at a Relay Node

The connection release procedure is initiated at a relay node by the SCCP or by reception of an *RLSD* message on a connection section.

3.3.4.1 Initial Actions

When an *RLSD* message is received on a connection section, the following actions then take place:

1. A *RLC* message is transferred on the connection section, the resources associated with the connection are released and the local reference number is frozen;
2. A *RLSD* message is transferred on the associated connection section; the reason is identical to the reason in the received message;
3. If the connection was established using a REQUEST interface element, then an N-DISCONNECT indication primitive is invoked;
4. The release timer, T(rel), is started on the associated connection; and
5. The inactivity control timers, T(ias) and T(iar), if still running, are stopped on both connection sections.

When the connection release procedure is initiated by the SCCP at a relay node during the data transfer phase, the following actions take place on both of the connection sections:

1. A *RLSD* message is transferred on the connection section;
2. If the connection section was established using an interface element, then an N-DISCONNECT indication primitive is invoked;
3. The release timer, T(rel), is started;
4. The inactivity control timers, T(ias) and T(iar), if still running, are stopped.

3.3.4.2 Subsequent Actions

The following actions are performed at a relay node during connection release:

1. When a *RLC* or *RLSD* message is received on a connection section, the resources associated with the connection are released, the T(rel) is stopped, and the local reference number is frozen; and
2. When the release timer expires, a *RLSD* message is transferred on the connection section. The sending of the *RLSD* message is repeated periodically.

When the T(rel) timer expires, T(int) and T(repeat rel) timers are started. A *RLSD* message is transferred on the connection section. When T(repeat rel) expires during the duration of T(int), it is restarted. An *RLSD* message is sent each time T(repeat rel) is restarted. Note that if congestion occurs, a longer value of T(repeat rel) might be applied.

When T(int) expires, stop T(repeat rel) if still running, release connection resources, and freeze the local reference number.

3.3.5 Actions at an End Node Not Initiating Connection Release

When a *RLSD* message is received at an end node of a signaling connection, the following actions are performed on the connection section:

1. A *RLC* message is sent on the connection section;
2. The resources associated with the connection section are released, the SCCP user is informed that a release has occurred by invoking the N-DISCONNECT indication primitive, and the local reference number is frozen; and
3. The inactivity control timers, T(ias) and T(iar), if still running, are stopped.

3.4 Inactivity Control

The purpose of the inactivity control is to recover from:

1. Loss of a *CC* message during connections establishment;
2. The unsignaled termination of a connection section during data transfer; and
3. A discrepancy in the connection data held at each end of a connection.

Two inactivity control timers, the receive inactivity control timer T(iar) and the send inactivity control timer T(ias), are required at each end of a connection section. The length of the receive inactivity timer must be longer than the length of the longest inactivity timer in the surrounding nodes. It might be advantageous to make sure that the inactivity receive timer T(iar) is at least twice the inactivity send timer T(ias). This avoids the loss of one single *IT* message (e.g., due to short term MTP congestion) causing the inadvertent release of an otherwise inactive SCCP connection. Loss of more messages (e.g., due to SP failure) will however still cause the connection to be released.

When any message is sent on a connection section, the send inactivity control timer is reset.

When any message is received on a connection section, the receive inactivity control timer is reset.

When the send inactivity timer, T(ias), expires, an *IT* message is sent on the connection section.

The receiving SCCP checks the information contained in the *IT* message against the information held locally. If a discrepancy is detected, the following actions (Table 1/ATIS-1000112.4) are taken:

Table 1/ATIS-1000112.4 - Actions for Discrepancies between an Inactivity Test Message and Local Data

Discrepancy	*Action*
Source reference number	Release connection
Protocol class	Release connection
Sequencing/segmenting*	Reset connection
Credit*	Reset connection

NOTE - *- Does not apply to class 2 connection.

When the receive inactivity control timer, T(iar), expires, the connection release procedure is initiated on a temporary connection section and OMAP is informed for a permanent connection section.

3.5 Data Transfer

3.5.1 General

The purpose of data transfer is to provide the functions necessary to transfer user information on a temporary or permanent signaling connection.

3.5.1.1 Actions at the Originating Node

The SCCP user at the originating node requests transfer of user data on a signaling connection by invoking the N-DATA request primitive.

The *DT* message is then generated, which must be transferred on the connection section. If flow control procedures apply to the connection section, these procedures must be enacted before the message can be forwarded on the connection section.

3.5.1.2 Actions at a Relay Node

If a signaling connection consists of more than one connection section, then one or more relay nodes are involved in the transfer of *DT* messages on the signaling connection.

When a valid *DT* message is received on an incoming connection section at a relay node, the associated outgoing connection section is determined. The relay node then forwards the *DT* message to the associated outgoing connection section for transfer to the distant node. If flow control procedures apply to the connection sections, then the appropriate procedures must be enacted on both connection sections. On the incoming connection section, these procedures relate to the reception of a valid *DT* message; on the outgoing connection section, the procedures control the flow of *DT* messages on the connection section.

3.5.1.3 Actions at the Destination Node

When the destination node receives a valid *DT* message, the SCCP user is notified by invoking the N-DATA indication primitive. If flow control procedures apply to the signaling connection, the flow control procedures relating to the reception of a valid *DT* message are enacted.

3.5.2 Flow Control

3.5.2.1 General

The flow control procedures apply during data transfer only, and are used to control the flow of *DT* messages on each connection section.

The flow control procedures apply only to protocol class 3.

The reset procedure causes reinitialization of the flow control procedure.

The expedited data procedure is not affected by this flow control procedure.

3.5.2.2 Sequence Numbering

For protocol class 3, for each direction of transmission on a connection section, the *DT* messages are numbered sequentially.

The sequence numbering scheme of the *DT* messages is performed modulo 128 on a connection section.

Upon initialization or reinitialization of a connection section, message send sequence numbers, P(S), are assigned to *DT* messages on a connection section beginning with P(S) equal to 0. Each subsequent *DT* message sequence number is obtained by incrementing the last assigned value by 1. The sequence numbering scheme assigns sequence numbers up to 127.

3.5.2.3 Flow Control Window

A separate window is defined, for each direction of transmission, on a connection section in order to control the number of *DT* messages authorized for transfer on a connection section. The window is an ordered set of W consecutive message send sequence numbers associated with the *DT* messages authorized for transfer on the connection section.

The lower window edge is the lowest sequence number in the window.

The sequence number of the first *DT* message not authorized for transfer on the connection is the value of the lower window edge plus W.

The maximum window size is set during connection establishment for temporary connection sections. For permanent connection sections, the window size is fixed at establishment. The maximum size shall not exceed 127.

Negotiation procedures during connection establishment allow for the negotiation of the window size.

3.5.2.4 Flow Control Procedures

3.5.2.4.1 Transfer of DT 2 Messages

If flow control procedures apply to a connection section, then all *DT2* messages on the connection section contain a send sequence number, P(S), and a receive sequence number, P(R). The procedure for determining the send sequence number to be used in a *DT2* message is described in clause 3.5.2.2. The receive sequence number, P(R), is set equal to the value of the next send sequence number expected on the connection section and P(R) becomes the lower window edge of the receiving window.

An originating or relay node is authorized to transmit a *DT2* message if the message send sequence number of the message is within the sending window -- that is, if P(S) is greater than or equal to the lower window edge and less than the lower window edge plus W. When the send sequence number of a *DT2* message is outside of the sending window, the node is not authorized to transmit the message.

3.5.2.4.2 Transfer of AK Messages

AK messages may be sent when there are no *DT2* messages to be transferred on a connection section.[9]

When a node transfers an *AK* message on a connection section, it is indicating that the node is ready to receive W *DT2* messages within the window starting with the receive sequence number, P(R), found in the *AK* message. That is, P(R) is the next send sequence number expected at the remote node on the connection section. Furthermore, P(R) also becomes the lower window edge of the receiving window.

An *AK* message must be sent when a valid *DT2* message -- as per clause 3.5.2.4.3 on P(S) and P(R) -- is received, P(S) is equal to the upper edge of the receiving window, and there are no *DT2* messages to be transferred on the connection section. Sending of *AK* messages before having reached the upper edge of the receiving window is also allowed during normal operation.

AK messages may also be sent by a node encountering congestion on a connection section as described below.

Assuming nodes X and Y are the two ends of a connection section, the following procedures apply:

- When a node Y experiences congestion on a connection section, it informs the remote node X using the *AK* message with the credit set to zero.
- Node X stops transferring *DT2* messages on the connection section.
- Node X updates the window on the connection section using the value of the received sequence number, P(R), in the *AK* message.
- Node X begins transfer of *DT2* messages when it receives an *AK* message with a credit field greater than zero, or when an *RSR* message is received on a connection section for which an *AK* message with a credit field equal to zero had previously been received.
- Node X updates the window on the connection section using the credit value. The credit value in an *AK* message must either equal zero or equal the initial credit agreed to at connection establishment.

3.5.2.4.3 Reception of a Data or AK Message

When a relay or destination node receives a *DT2* message, it performs the following test on the send sequence number, P(S), contained in the *DT2* message:

1. If P(S) is the next send sequence number expected and is within the window, then the node accepts the *DT2* message and increments by one the value of the next sequence number expected on the connection section;
2. If P(S) is not the next send sequence number expected, then the reset procedure is initiated on the connection section;

[9] Further study is required to determine criteria to be used to decide when *Data Acknowledgement* messages are sent for cases other than the congestion situation described in this section.

3. If P(S) is not within the window, then this is considered a local procedure error and the connection reset procedure is initiated; and
4. If P(S) is not equal to 0 for the first *DT2* message received after initialization or reinitialization of the connection section, this is considered a local procedure error and the connection reset procedure is initiated.

The message receive sequence number, P(R), is included in *DT2* and *AK* messages. When a node receives a Data or *AK* message on a connection section, the value of the receive sequence number, P(R), implies that the remote node has accepted at least all *DT2* messages numbered up to and including P(R) - 1. That is, the next expected send sequence number at the remote node is P(R). The receive sequence number, P(R), contains information from the node sending the message, which authorized the transfer of a limited number of *DT2* messages on the connection section. When a node receives a *DT2* or *AK* message:

a) The receive sequence number, P(R), contained in the message becomes the lower window edge of the sending window:
    1) If the value of P(R) is greater than or equal to the last P(R) received by the node on that connection section; and
    2) If the value of the received P(R) is less than or equal to the P(S) of the next *DT2* message to be transferred on that connection section.
b) The node initiates the reset procedure on the connection section if the receive sequence number, P(R), does not meet conditions 1) and 2) under a).

3.5.3 Segmenting and Reassembly

During the data transfer phase, the N-DATA request primitive is used to request transfer of octet - aligned data (NSDUs) on a signaling connection. NSDUs longer than 255 octets must be segmented before insertion into the "data" field of a *Data Form 1/2* message.

The more - data indicator (M-bit) is used to reassemble an NSDU that has been segmented for conveyance in multiple *DT* messages. The M-bit is set to 1 in all Data Form 1/2 messages except the last message whose data field relates to a particular NSDU. In this way, the SCCP can reassemble the NSDU by combing the data fields of all *DT* messages with the M-bit set to 1 with the following Data Form 1/2 message with M-bit set to 0. The NSDU is then delivered to the SCCP user using the N-DATA indication. *DT* messages in which the M-bit is set to 1 do not necessarily have the maximum length.

Segmentation and reassembly are not required if the length of the NSDU is less than or equal to 255 octets.

3.6 Expedited Data Transfer

3.6.1 General

The expedited data procedure applies only during the data transfer phase and is applicable to protocol class 3.

For the case of expedited data transfer, each message contains one NSDU, and no segmenting and reassembly is provided.

If an *ED* or *EA* message is lost, then subsequent *ED* messages cannot be forwarded on the connection section.

3.6.2 Actions at the Originating Node

The expedited data transfer procedure is initiated by the user of the SCCP using the N-EXPEDITED-DATA request primitive, which contains up to 32 octets of user data.

When the SCCP user invokes the N-EXPEDITED-DATA request primitive, an *ED* message with up to 32 octets of user data is transferred on the connection section once all previous *ED* messages for the connection section have been acknowledged.

3.6.3 Actions at a Relay Node

Upon receiving a valid *ED* message, a relay node confirms this message by transferring an *EA* message on the incoming connection section. Withholding of the *EA* message is a means of providing flow control of *ED* messages.

If a node receives another *ED* message on the incoming connection section before sending the *EA* message, the node shall discard the subsequent message and reset the connection.

The relay node determines the associated outgoing connection section. An *ED* message is then transferred on the associated outgoing connection section, once all previous *ED* messages on that connection section have been acknowledged.

The *EA* message must be sent before acknowledging subsequent *DT* or *ED* messages received on the incoming connection section.

3.6.4 Actions at the Destination Node

The destination node of the connection section confirms a valid *ED* message by transferring an *EA* message on the connection section. Withholding of the *EA* message is a means of providing flow control of *ED* messages.

If a node receives another *ED* message on a connection section before sending the *EA* message, then the node shall discard the subsequent message and reset the connection.

The destination node then invokes the N-EXPEDITED DATA indication primitive.

The N-EXPEDITED-DATA indication must be issued to the SCCP user at the destination node before N-DATA or N-EXPEDITED-DATA indications resulting from any subsequently issued N-DATA or N-EXPEDITED-DATA requests at the originating node of that signaling connection. The initiation of the *EA* message is implementation dependent.

3.7 Reset

3.7.1 General

The purpose of the reset procedure is to reinitialize a connection. It is applicable only to protocol class 3. It is noted that the time sequence of the primitives in the reset procedure may be varied as long as it is consistent with ITU-T Recommendation X.213.

For a connection reset initiated by the SCCP, *DT* or *ED* messages shall not be transferred on the connection section prior to the completion of the reset procedure.

3.7.2 Action at an End Node Initiating the Reset Procedure

3.7.2.1 Initial Actions

When a connection reset is initiated in an end node, by the SCCP user invoking an N-RESET request primitive or by the SCCP itself, the following actions are performed at the initiating node:

1. An *RSR* message is transferred on the connection section;
2. The send sequence number, P(S), for the next *DT* message is set to 0. The lower window edge is set to 0. The window size is reset to the initial credit value;
3. The SCCP user is informed that a reset has taken place by:
    - ♦ Invoking the N-RESET indication primitive if the reset is network originated.
4. The reset timer T (reset) is started;
5. Pending expedited data processes must be cleared; and
6. *All DT2, AK, ED* and *EA* messages waiting for transmission are discarded.

3.7.2.2 Subsequent Actions

The following actions are performed at the initiating node on a connection section for which an *RSR* message has been previously transferred:

1. When a *DT*, *AK*, *ED* or *EA* message is received, the message is discarded. When an N-DATA request or N-EXPEDITED DATA request primitive is received, the primitive is discarded or stored up to the completion of the reset procedure. The choice between these two is implementation dependent;
2. When the reset timer expires, the connection release procedure is initiated on a temporary connection section, and OMAP is informed for a permanent connection section;
3. When an *RSC* or an *RSR* message is received on the connection section, the reset is completed provided the SCCP has previously received an N-RESET request or response primitive from the SCCP user, and (therefore) data transfer is resumed, and the timer T(reset) is stopped. The SCCP user is informed that the reset is completed by invoking the N-RESET confirmation primitive; and
4. When an *RLSD* message is received on a temporary connection section, the release procedure is initiated and the timer, T (reset), is stopped.

3.7.3 Actions at a Relay Node

3.7.3.1 Initial Actions

The connection reset procedure is initiated at the relay node, either by the SCCP at the node itself or by the reception of an *RSR* message.

When a *RSR* message is received on a connection section, the following actions take place:

1. A *RSC* message is transferred on the connection section;
2. A *RSR* message is transferred on the associated connection section; the reason for reset is identical to the reason in the *RSR* message;
3. On both the connection section and the associated connection section, the send sequence number, P(S), for the next *DT* message to be transmitted is set to 0, and the lower window edge is set to 0. The window size is reset to the initial credit value on both connection sections;
4. The data transfer procedure is initiated on the connection section;
5. The reset timer, T (reset), is started on the associated connection section;
6. Pending expedited data processes must be cleared; and
7. All DT2, *AK, ED* and *EA* messages waiting for transmission are discarded.

When the connection reset procedure is initiated by the SCCP at the relay node, the following actions take place on both of the connection sections:

1. A *RSR* message is transferred;
2. The send sequence number, P(S), for the *DT* message is set to 0. The lower window edge is set to 0. The window size is reset to the initial credit value; and
3. The reset timer T (reset) is started.

3.7.3.2 Subsequent Actions

If the connection reset was initiated by reception of an *RSR* message on a connection section, then the following actions are performed after initial actions are completed:

1. When a *DT*, *AK, ED*, *EA* message is received on the associated connection section, the message is discarded;
2. When the reset timer expires on the associated connection section, the connection release procedure is initiated on a temporary connection section, and the maintenance function is alerted on permanent connection section;
3. When a *RLSD* message is received on a temporary connection section, the connection release procedure is initiated, and the timer, T (reset), is stopped; and
4. When a *RSC* or *RSR* message is received on the associated connection section, the data transfer procedure is resumed, and the timer, T (reset), is stopped.

If the connection reset was initiated by the SCCP at the relay node, then the following actions are performed once the initial actions are completed:

1. When a *DT*, *AK*, *ED*, *EA* message is received on either connection section, the message is discarded;
2. When the reset timer expires on a temporary connection section, the connection release procedure is initiated and on a permanent connection a maintenance function is alerted;
3. When an *RLSD* message is received on a temporary connection section, then the connection release procedure is initiated, and the reset timer, T (reset), is stopped; and
4. When an *RSC* or *RSR* message is received on a connection section, data transfer is resumed on that connection, and the timer, T (reset), is stopped.

3.7.4 Actions at an End Node Not Initiating the Reset Procedure

When an *RSR* message is received at an end node, the following actions are performed on the connection section:

1. The send sequence number, P(S), for the next *DT* message is set to 0, the lower window edge is set to 0. The window size is reset to the initial credit value;
2. The SCCP user is informed that a reset has occurred by invoking the N-RESET indication primitive;
3. A *RSC* message is transferred on the connection section after an N-RESET response or request primitive is invoked by the user; and
4. An N-RESET confirmation primitive is invoked to inform the SCCP user that the reset is completed and the data transfer can be resumed.

3.7.5 Handling of Messages During the Reset Procedures

Once the reset procedure is initiated, the following actions are taken with respect to *DT* messages:

- Those that have been transmitted, but for which an acknowledgment has not been received, are discarded;
- Those that have not been transmitted, but are contained in an M-bit sequence for which some *DT* messages have been transmitted, are discarded; and
- Those *DT* messages that have been received, but which do not constitute an entire M-bit sequence, are discarded.

3.8 Restart

3.8.1 General

The purpose of the restart procedure is to provide a recovery mechanism for signaling connection sections in the event of a node failure.

3.8.2 Actions at the Recovered Node

3.8.2.1 Initial Actions

When a node recovers from its failure, the following actions are performed:

1. A guard timer, T(guard)[10] is started;
2. If the recovered node has knowledge about the local reference numbers in use before failure, then the normal procedures for temporary signaling connections are resumed with the assumption that the local reference number that were in use before the node failure are not assigned, at least during T(guard); and
3. A maintenance function is informed for the re-establishment of permanent signaling connections.

3.8.2.2 Subsequent Actions

The following actions are performed at the recovered node, on every temporary signaling connection section if the node does not know the local reference numbers in use before failure, or only on the temporary signaling connection sections in operation before failure if the node has such knowledge:

a) Before the guard timer, T(guard), expires:
   1) When a *RLSD* message is received with both source and destination local reference numbers, a *RLC* message, with reversed local reference numbers, is returned to the originating point code.
   2) Any other connection-oriented messages received are discarded.

b) When the guard timer, T(guard), expires normal procedures are resumed.

3.8.3 Actions at the Non-Failed Far End Node

The inactivity control procedure, described in clause 3.4, is used by the non-failed far end node to recover from the unsignaled termination of a connection section during data transfer.

3.9 Permanent Signaling Connections

Permanent signaling connections are set up administratively, and connection establishment procedures and connection release procedures are not initiated by the SCCP user.

Permanent signaling connections are realized using one or more connection sections.

A permanent signaling connection is either in the data transfer phase or the reset phase. Therefore, all procedures relating to the data transfer phase for connection-oriented protocol classes and the reset procedures are applicable to permanent signaling connections.

---

[10] The guard timer must be large enough, so that all the non-failed far end nodes can detect the failure and can safely release the affected temporary signaling connection sections. This implies T(guard) > T(iar) + T(int) + T(rel).

3.10 Abnormalities

3.10.1 General

Errors can be classified into the three categories listed below. Examples of each category are included for clarification:

1. *Syntax errors* - in general, two kinds of syntax errors can be distinguished:
   a. Value errors - Invalid values for a single information element that lead to the impossibility to decode the message;
   b. Construction errors - Errors in the sequence or length of information elements or inconsistencies between announced and actual contents of an information element.

   For SCCP, the following errors could be considered as syntax errors:

   a. *Value errors*:
      - ♦ a1 A unknown message type;
      - ♦ a2 A invalid value of protocol class;
      - ♦ a3 Invalid value of global title indicator;
      - ♦ a4 Invalid value for the encoding scheme;
      - ♦ a5 Unassigned local reference number.

      All other "value errors" are not considered as syntax failures. They are either ignored (as spare fields or spare values) or treated as (unknown) routing failures. The former four errors make it impossible to treat the message in any sensible way and are therefore syntax errors.

   b. *Construction errors*:
      - ♦ b1 Minimum and maximum length of a parameter according to ATIS-1000112.3 is not respected;
      - ♦ b2 Pointers to variable or first optional parameter point beyond end of message;
      - ♦ b3 Length of an optional parameter extends beyond end of message (may be because EOP is forgotten);
      - ♦ b4 The combination of pointer values and length of parameters (or sum of length of optional parameters) results in overlapping parameters;
      - ♦ b5 Length of a calling or called party address is not compatible with contents as indicated in the address indicator of the address;
      - ♦ b6 In an address, no SSN is included, although the routing indicator indicates "Route on SSN";
      - ♦ b7 In an address, no GT is included although the routing indicator indicates "Route on GT" (except as indicated in ATIS-1000112.3, clause 3.5).

2. *Logical errors* - This type of error occurs when a node receives a message that is not an acceptable input to the current state of the connection section, or whose value of P(S) or P(R) is invalid. Examples of logical errors are:
   - ♦ Reception of an acknowledgment message when the corresponding request message has not been sent;
   - ♦ Reception of a *DT* message whose data field length exceeds the maximum data field permitted on the connection section;
   - ♦ Reception of a second *ED* message before an *EA* message has been sent, and;
   - ♦ Reception of message whose value of P(R) is not greater than or equal to the last P(R) received and is not less than or equal to the next value of P(S) to be transmitted.
3. *Transmission errors* - This type of error occurs when a message is lost or delayed. An example of transmission error is:
   - ♦ Expiration of a timer before reception of the appropriate acknowledgment message.

3.10.2 Syntax Error

When syntax errors are detected (see clause 3.10.1) in a connection-oriented message, the message is discarded. Checking syntax errors beyond the processing required for the SCCP connection-oriented message routing is not mandatory.

3.10.3 Action Tables

The action tables found in ATIS-1000112.4, Annex B, include information -- in addition to that found in the text of ATIS-1000112.4 -- regarding the actions to be performed upon receipt of a message. In particular, these tables are helpful in determining the actions to be performed upon receipt of a message resulting in a logical error.

3.10.4 Actions Upon the Reception of an ERR Message

Upon the reception of an *ERR* message at a node, the following actions are performed on the connection section for error causes other than "service class mismatch":

1. The resources associated with the connection are released; and
2. The local reference number is frozen (see clause 3.3.2).

Upon the reception of a *ERR* message at a node with the error cause "service class mismatch," the connection release procedure is initiated by the SCCP at the node (see clause 3.3).

4 CONNECTIONLESS PROCEDURES

This clause specifies the requirements SCLC and SCRC shall meet for the support of connectionless procedures with protocol classes 0 and 1, and how the elements for layer to layer communication shall be used.

It is the objective to operate the connectionless protocol in various SCCP network environments.

These may be:

1. An environment with only MTP network(s) supporting 272-octet MTP-SDU sizes;
2. An environment with MTP network(s) supporting 4095-octet MTP-SDU sizes; or
3. A mixed environment of interworking case 1 and 2.

All environments must support all SCCP management messages.

An implementation shall support all message types, parameters, and parameters values (see ATIS-1000112.3) applicable to the connectionless protocol classes and capabilities of this standard, but the network may allow lesser functionality according to its situation in the network(s) in which it is required to operate.

The connectionless procedures allow a user of the SCCP transfers up to 2560 - 3904[11] octets of user data without first requesting establishment of a signaling connection.

The N-UNITDATA request and indication primitives are used by the user of the SCCP to request transfer of user data by the SCCP and for the SCCP to indicate delivery of user data to the destination user. Parameters associated with the N-UNITDATA request primitive must contain all information necessary for the SCCP to deliver the user data to the destination.

Transfer of the user data is accomplished by including the user data in *UDT/XUDT/LUDT* messages.

When the user of the SCCP requests transfer of user data by issuing an N-UNITDATA request primitive, there are two classes of service that can be provided by the SCCP: protocol classes 0 and 1. These protocol classes are distinguished by their message sequencing characteristics.

When the user of the SCCP requests transfer of several messages by issuing multiple N-UNITDATA request primitives, the probability of these messages being received in sequence at the Called Address depends on the protocol class designated in the request primitives. For protocol class 0, the sequence control parameter is not included in the N-UNITDATA request primitive and the SCCP may generate a different SLS for each of these messages. For protocol class 1, the sequence control parameter is included in the N-UNITDATA request primitive, and -- if the parameter is the same in each request primitive -- then the SCCP will generate the same SLS for these messages.

The MTP retains message sequencing for those messages with the same SLS field. The SCCP relies on the services of the MTP for transfer of SCCP messages. Based on the characteristics of the MTP, the protocol class 1 service may be used in such a way that it provides a quality of service that has a lower probability of out-of-sequence messages than that provided by protocol class 0.

UDT/XUDT/LUDT protocol class 1 messages with a particular SLS code received at a destination from the MTP by the SCCP for a particular SCCP user should be delivered to the user in the same order in which they were received from the MTP.

---

[11] Maximum value depends on the length of the called and calling party addresses, and on whether or not segmentation may occur (3904 = [251 - 7] * 16, where 251 is the user data length fitting in one *XUDT*, 16 the maximal number of segments and 7 the length of the optional parameter: "segmentation" followed by the end of optional parameters octet.)

UDT/XUDT/LUDT protocol class 1 messages with a particular SLS code received at an SCCP relay point from the MTP by the SCCP for a particular SCCP user should be delivered to the MTP in the same order as they are received from the MTP, and there should be a fixed mapping from the SLS code in the received messages to the SLS code in the transmitted messages.

4.1 Data Transfer

The N-UNITDATA request primitive is invoked by the SCCP user at an originating node to request connectionless data transfer service. The connectionless data transfer service is also used to transport SCCP management messages, which are transferred in the user data field of *UDT/XUDT/LUDT* messages.

The user data is then transferred in *UDT/XUDT/LUDT* message(s), using SCCP and MTP routing functions, to the Called Address indicated in the N-UNITDATA request primitive.

SCCP routing and relaying functions may be required at intermediate nodes, since complete translation and routing tables for all addresses are not required at every node.

When the user data can not be transferred to its destination, the message return function is initiated.

The SCCP uses the services of the MTP; the MTP may, under severe network conditions, discard messages. Therefore, the user of the SCCP may not always be informed of non-delivery of user data. The MTP notifies the SCCP of unavailable or congested signaling points using the MTP-PAUSE indication or MTP-STATUS indication, respectively. If SCCP Flow Control is chosen as an option (see clause 5.5), the MTP will also use the MTP-STATUS to notify the SCCP of an unavailable SCCP.

When a *UDT/XUDT/LUDT* message is received at the destination node, an N-UNITDATA indication primitive is invoked. Because SCCP management messages are transferred using the connectionless data transfer service, they must be identified prior to invoking the N-UNITDATA primitive.

4.1.1 Segmentation/Reassembly

4.1.1.1 Segmentation

4.1.1.1.1 General

The connectionless segmentation mechanism is provided by the SCLC block. It is used in two situations:

1. When a SCCP user generates an N-UNITDATA request primitive, and SCLC is able to segment the message before passing it to SCRC; and
2. When the compatibility test in SCRC sends a message to SCLC for segmentation.

The actions of SCLC depend on the length of the user data as follows:

- ♦ If the length of the user data is lower than X octets, then SCLC shall avoid segmentation and an *UDT/XUDT/LUDT* message is passed to SCRC.

- If the length of the user data is between X and Y octets[12], then the SCCP may decide to segment the message, based on locally stored information regarding network performance and configuration.
- If the length of the user data is between Y and 3904 octets inclusive, then the SCCP shall segment the message.
- If the length of the user data is greater than 3904 octets, then the error treatment shall apply.

4.1.1.1.2 Normal Procedures

If the SCCP determines that segmentation is needed, it should break the original block of user data into smaller blocks of data that can be carried as user data in *XUDT* messages (the use of *LUDT* messages for this purpose is for further study). The size of the segments should be chosen so that a minimum number of segments is sent, subject to local knowledge of the network status. A maximum of 16 segments should be sent for one N-UNITDATA request primitive. The size of the first segment should be selected so that the total message size is less than or equal to the size of the first segment multiplied by the number of segments. This provides for an effective buffer management capability at the destination SCCP.

After breaking the user data into smaller segments, the SCCP should form a sequence of *XUDT* messages as described below:

- The SCCP should place each segment of user data into separate *XUDT* messages, each with the same Calling Party Address and identical MTP routing information;
- The Calling Party Address and the OPC in each *XUDT* message should be coded identically, in the manner described in clause 2.1, SCCP Addressing;
- Each segmented *XUDT* message should include the segmentation parameter;
- The Segment Number field of the segmentation parameter should be coded with the remaining number of segments in the segmentation process; for example, in the first segment, this field should be set to one less than the total number of segments;
- The allocation of the Segmentation Local Reference value shall use one of the following procedures:
  - The value of the Segmentation Local Reference field should cycle through all possible values sequentially that can be represented by the 24 bits allocated; or
  - The Segmentation Local Reference field of the segmentation parameter should be coded with a unique local reference that should remain frozen for time T(fr)[13]. In the case where segmentation follows the reception of an *LUDT* message, then the Segmentation Local Reference put in each segment shall be identical to the Segmentation Local Reference received in the segmentation parameter of this corresponding *LUDT* message. If the segmentation parameter was not present in the received *LUDT* message, then the message return procedure is initiated with the return cause “segmentation failure”;

---

[12] The exact specification of the X and Y values is for further study.

[13] The value for timer T(fr) is implementation dependent.

- The F-bit in the first segment should be coded as one; the F-bit in each remaining segment should be coded as zero;
- The protocol class for each segmented *XUDT* message should be set to one. At the originating node, the In-Sequence Delivery Option field of the segmentation parameter should be set as indicated in the N-UNITDATA request primitive. If the segmentation is performed at a relay node, the In-Sequence Delivery Option field shall be set in each segment to the value of the protocol class received in the incoming message; and
- When an N-UNITDATA request primitive results in a single *LUDT* message, but there is a possibility that the data parameter will be segmented at an SCCP relay node, then the segmentation parameter is included in the message.

4.1.1.1.3 Return on Error Procedures

If message return is requested by the SCCP user, then it is an implementation decision that determines which *XUDT/LUDT* messages have return on error requested. If an *XUDTS* message is later received, then it is an implementation decision that determines how the SCCP should deal with the returned *XUDTS/LUDTS* message.

When the return option is set to return message on error in a received *LUDT* message and this message is segmented, the return option will only be set in the first segment.

The following errors may occur during segmenting:

- Segmentation not supported; or
- Segmentation failed.

4.1.1.1.3.1 Segmentation non supported

An *LUDT* message arrives at an interworking node, and the segmentation function is not implemented:

The following cause applies:

- *Return Cause*: Segmentation non supported.

4.1.1.1.3.2 Segmentation failed

An *LUDT* message arrives at an interworking node, and the segmentation fails for lack of resources or another transient condition in the interworking node.

The following cause applies:

- *Return Cause*: Segmentation failed.

4.1.1.2 Reassembly

4.1.1.2.1 General

Upon receipt of an *XUDT/LUDT* message with the F-bit set to one in the segmentation parameter, the destination SCCP should initiate a new reassembly process using the Calling Party Address and Segmentation Local Reference -- together with MTP routing information -- to uniquely identify the reassembly process.

Initiating a reassembly process involves the following steps:

- The SCCP should start the reassembly timer, T(reassembly). If the reassembly timer expires before all segments are received and reassembled, then the SCCP should discard the message and stop the reassembly process;
- The SCCP should determine the upper bound on the total message length by multiplying the length of the first segment by one more than the number of remaining segments indicated in the segmentation parameter of the first segment; and
- The SCCP should extract the user data of the segment and buffer it, so that it can be concatenated with subsequent segments.

Further study is needed to determine the actions required when an *XUDT/LUDT* message is received with the F-bit set to one, referring to an already existing reassembly process.

4.1.1.2.2 Normal Procedures

Upon receipt of an *XUDT/LUDT* message with the F-bit set to zero in the segmentation parameter, the SCCP should perform the following steps when reassembling the message.

- The SCCP should associate the received *XUDT/LUDT* message with a particular reassembly process, using the unique combination of the Calling Party Address, MTP routing information, and the Segmentation Local Reference field of the segmentation parameter. If no association is possible, the SCCP should discard the message;
- The SCCP should verify that the segment is received in sequence by examining the Remaining Segments field of the segmentation parameter, which should be one less than the previous segment. If a segment is received out of sequence, or a duplicate segment is received, then the SCCP should initiate the return on error procedure. The received segments are discarded;
- The SCCP should extract the user data of the segment and concatenate it with the other segments, in the order received. Segments can be any length, and not all segments of a particular segmentation process need to be the same length. Thus, the destination SCCP should be able to deal with segments of any length; and
- When the Remaining Segments field of the segmentation parameter is zero, and all segments are properly assembled, the SCCP should pass the message to the appropriate SCCP user as user data in an N-UNITDATA indication primitive. The destination SCCP should examine the In-Sequence Delivery Option field of the segmentation parameter to determine if sequencing is needed between the reassembled message and any other received message, since the protocol class will always be set to one in a XUDT/LUDT segment.

4.1.1.2.3 Return on Error Procedures

If an error occurs during reassembly, the SCCP can return an *XUDTS/LUDTS* message containing a "first" segment of user data, if return on error was requested in an *XUDT/LUDT* message received as part of the reassembly process. The amount of user data contained in the message is an implementation decision, but it should correspond to the first block or blocks of user data received. In some cases this will be the first segment transmitted by the segmentation process, but in other situations, it will not.

The reassembly function will never change the segment number of the segments to be returned. No specific indication will be given that there is only a "first" segment.

4.1.2 Message Change

When the compatibility test in SCRC sends a message to SCLC to change the message type, SCLC should pass a message of the requested type, containing all the parameters of the received message, to SCRC.

The insertion of optional parameters without message type change is permitted, their values may be network dependent. Where an optional parameter is present in a message received at an interworking node, and the resulting outgoing message is of the same type, then the optional parameter may either be deleted or its value transcribed according to the need of the outgoing network. Such parameter manipulation can also occur when the message type changes.

Where interworking between narrowband and broadband environment exists, the only required format conversions are the following:

- ♦ *LUDT* ---> *XUDT* (1-N segments, message type change with or without segmentation); and
- ♦ *LUDTS* ---> *XUDTS* (message type change and truncation).

The other allowed format conversions are the following (optional):

- ♦ *LUDT* ---> *LUDT* (2-N segments, no message type change but segmentation);
- ♦ *XUDT* ---> *LUDT* (message type change without reassembly);
- ♦ *LUDTS* ---> *XUDTS* (message type change without truncation);
- ♦ *XUDTS* ---> *LUDTS* (message type change without truncation);
- ♦ *UDT* ---> *XUDT* (1-N segments, message type change with or without segmentation; see clause 4.1.2.1 *UDT(S)/XUDT(S)* Message Change Procedures);
- ♦ *XUDT* ---> *UDT* (see clause 4.1.2.1 *UDT(S)/XUDT(S)* Message Change Procedures);
- ♦ *UDTS* ---> *XUDTS* (message type change with possible truncation; see clause 4.1.2.1 *UDT(S)/XUDT(S)* Message Change Procedures); and
- ♦ *XUDTS* ---> *UDTS* (message type change; see clause 4.1.2.1 *UDT(S)/XUDT(S)* Message Change Procedures).

Other format conversions are for further study.

4.1.2.1 *UDT(S) / XUDT(S)* Message Change Procedures

The *UDT(S)* to *XUDT(S)* and *XUDT(S)* to *UDT(S)* message change procedures are functions in an SCCP relay node. The message change procedures enable interworking between the end nodes with different message handling capability.

4.1.2.1.1 SCCP Relay Node

4.1.2.1.1.1 *UDT(S) to XUDT(S)* Message Change

At an SCCP relay node with the message change capability, the compatibility test in SCRC may request a *UDT(S)* to *XUDT(S)* message change from SCLC. Following rules apply for *UDT(S)* to *XUDT(S)* message change procedures:

- ♦ An *UDT(S)* to *XUDT(S)* message change should only occur if the GTT result is non-final and the message is destined to a node that is capable of receiving an *XUDT(S)* message.
- ♦ As an option, a Message Type Interworking parameter may be included in the *XUDT(S)* message. The Original Message Type field of the Message Type Interworking parameter, if present, will be set to indicate the original message type was *UDT(S)* before the message change.
- ♦ If the message change from an *UDT(S)* to *XUDT(S)* results in the maximum length of the Signaling Information Field (SIF) being exceeded as specified in ATIS-1000111.3, the message change is not allowed. If message change is not allowed, the message is forwarded as *UDT(S)* message.

4.1.2.1.1.2 *XUDT(S)* to *UDT(S)* Message Change

At an SCCP relay node with the message change capability, the compatibility test in SCRC may request an *XUDT(S)* to *UDT(S)* message change from SCLC. The following rules apply for *XUDT(S)* to *UDT(S)* message change procedures:

- ♦ *XUDT(S)* to *UDT(S)* message change is expected for *XUDT(S)* messages that are destined to nodes that are not capable of receiving *XUDT(S)* messages.
- ♦ Determination of whether an *XUDT(S)* message is allowed to be message changed to *UDT(S)* involves examination of each individual optional parameter. If a Segmentation[14] or ISNI parameter is present in the *XUDT(S)* message, message change to *UDT(S)* is not allowed. Unrecognized optional parameters may be dropped. If all the optional parameters can be dropped, the message change to *UDT(S)* is allowed.
- ♦ If the message change to *UDT(S)* is not allowed, then the SCCP must initiate return on error procedures.

---

[14] An *XUDT* message that is not a segmented message but contains a Segmentation parameter (i.e., F-bit set to "1" and number of remaining segments set to "0") will prevent the conversion of he message to a *UDT* message

4.1.2.1.2 *XUDT(S)* capable end node

An *XUDT(S)* capable end-node receiving the optional Message Type Interworking parameter may make use of the information to determine the appropriate message type for the response message. How it is done is implementation specific, and it is not within the scope of this document.

4.1.2.1.3 Message Change Error Procedures

The following Return Cause values are used for routing failures encountered due to message change procedures.

- *Message change failure*: Used when:
    - A message change processing error is encountered;
    - A data inconsistency is encountered during processing of the Message Type Interworking parameter.
- *Message incompatibility*: Used when:
    - A message cannot be changed because the message change functionality does not exist;
    - Cannot change XUDT(S) messages destined to a node that can only receive UDT messages (e.g., XUDT(S) messages containing segmentation parameter).

4.2 Message Return

The purpose of message return is to discard or return messages that encounter failures other than syntax errors (see clause 4.3), and cannot be delivered to their final destination.

The message return procedure is initiated if SCCP routing is unable to transfer a *UDT/XUDT/LUDT* or *UDTS/XUDTS/LUDTS* message, or if the SCCP can not segment or reassemble an *XUDT* message. The procedure may be initiated, for example, as a result of insufficient translation information or the inaccessibility of a subsystem or point code. Specific reasons are enumerated in clause 3.12 of ATIS-1000112.3.

1. If the message is a *UDT/XUDT/LUDT* message, and:
    a. The option field is set to return message on error, then a *UDTS/XUDTS/LUDTS* message is respectively transferred to the Calling Party Address.
    b. The option field is not set to return message on error, then the message is discarded.
2. If the undeliverable message is a *UDTS/XUDTS/LUDTS* message, it is discarded.

The user data field of the *UDT/XUDT/LUDT* message and the reason for return are included in the *UDTS/XUDTS/LUDTS* message.

When a *UDTS/XUDTS/LUDTS* message is received at the destination node, an N-NOTICE indication primitive is invoked.

In a mixed message environment, the message type used for the service message may not correspond with the message type of the failed message (e.g., an *UDTS* message may be used in response to a failed *XUDT* message). The node initiating the return on error procedures may use the information in the Message Type Interworking parameter if present and the received message type (*UDT* or *XUDT*) to determine the appropriate message type (*UDTS* or *XUDTS*) for the service message.

When the *XUDTS* message is the result of a routing failure of an *LUDT* message, which could only be returned in an *XUDTS*, the user data will be cut off to fit into one *XUDTS* message. When the *XUDTS* message is the result of a routing failure of the first *XUDT* segment resulting from segmenting an *LUDT* message, the user data will contain only the first segment of data.

4.3 Syntax Error

This type of error occurs when a node receives a message that it is unable to process because the message does not conform to the format specifications of the SCCP. Examples of syntax errors are:

1. Unreasonable pointer value (e.g., points beyond the end of the message);
2. Mismatch between message type and protocol class parameters;
3. Inconsistent address indicator and address contents; and
4. Unknown message type.

When a syntax error is detected for a connectionless message, the message is discarded.

If an *XUDTS/LUDTS* or *XUDT/LUDTS* message containing an unknown optional parameter is received, it is not considered a syntax error. If the SCCP is performing a relay function on the received message, the unknown optional parameter received is included in the outgoing message unchanged.

5 SCCP MANAGEMENT PROCEDURES

5.1 General

The purpose of SCCP management is to provide procedures to maintain network performance by rerouting or throttling traffic in the event of failure or congestion in the network.

Although SCCP management has its own subsystem number, the procedures in this clause do not apply to it except as specified in clause 5.5.

SCCP management is organized into three sub-functions: signaling point status management, subsystem status management, and traffic information management[15]. Signaling point status management and subsystem status management allow SCCP management to use information concerning the accessibility of signaling points and subsystems, respectively, to permit the network to adjust to failure, recovery, and congestion. Traffic information management provides a means for SCCP users to know received traffic patterns.

SCCP management procedures rely on: 1) failure, recovery, and congestion information provided in the MTP-PAUSE indication, MTP-RESUME indication and MTP-STATUS indication primitives, and 2)

[15] The Traffic Information Management procedures are optional.

subsystem failure, recovery and congestion information received in SCCP management messages[16]. SCCP management information is currently defined to be transferred using SCCP connectionless service with no return on error requested. Formats of these messages appear in ATIS-1000112.3.

The information pertaining to both single and replicated nodes or subsystems is used for SCCP management purposes. This allows Called Party Addresses that are specified in the form of a global title to be translated to different point codes and/or subsystem numbers depending on network or subsystem status.

Replicated nodes or subsystems may relate to their replicates in one of several ways. ("Replicate" is a term meaning one of a set of "multiple copies." A node or subsystem which is not replicated is termed "solitary.")

One mode uses a replicate in a dominant role. In the dominant mode, each replicate of a node/subsystem is associated with a priority. The combination of priority and accessibility status of the node/subsystem identifies the preferred node/subsystem. At any given time, the preferred node/subsystem is the accessible node/subsystem of highest priority. The procedures for the dominant mode assume that each replicate is associated with a unique priority.

In the dominant mode, traffic is split among several nodes/subsystems. Under normal conditions, each portion of the traffic is routed to the accessible node/subsystem of highest priority, which is the "preferred node/subsystem." When the current preferred node/subsystem becomes inaccessible, this traffic is routed to the accessible node/subsystem of the next highest priority, or the "next preferred node/subsystem." Thus, the accessible node/subsystem of next highest priority becomes the preferred node/subsystem. The "previously preferred node/subsystem" refers to the node/subsystem that was previously handling the traffic until either it became inaccessible, or until a higher priority node/subsystem became accessible. Upon node/subsystem recovery, it becomes the preferred node/subsystem, if it has higher priority that the node/subsystem currently handling the traffic.

Replicates can also operate in a loadshare mode[17]. Replicated nodes/subsystems operating in this mode are called “loadshare nodes/subsystems.” This procedure assumes that each loadshare node/subsystem is assigned equal priority.

In the loadshare mode, traffic is loadshared among several nodes/subsystems. Under normal conditions the traffic is distributed equally among the available loadshare nodes/subsystems. When a loadshare node(s)/subsystem(s) becomes inaccessible, the traffic is distributed equally among the remaining available loadshare nodes/subsystems. Upon the recovery of an inaccessible loadshare node(s)/subsystem(s) the traffic is distributed equally to all available loadshare nodes/subsystem.

Another mode uses a replicate in a replacement role. Consider two replicates, A and B, which are "alternatives." When A becomes inaccessible, its traffic is routed to B; but when A recovers, the traffic is not moved back to A. It is only when B becomes inaccessible that traffic is shifted back to A. In addition, other modes are possible.

The current SCCP management procedures are designed to manage solitary nodes/subsystems, and replicated nodes/subsystems that operate in a dominant mode, and replicated nodes/subsystems in the loadshare mode. Replicated nodes/subsystems may consist of any number of replicates.

---

[16] Subsystem congestion control is for further study.

[17] This procedure involves load sharing at the SCCP level and should not be confused with load sharing at the link level.

Management procedures for nodes/subsystems which operate in a mode other than the solitary, dominant, and loadshare mode and which have more than one backup, are for further study.

SCCP management procedures utilize the concept of a "concerned" subsystem or signaling point. In this context, a "concerned" entity means an entity with an immediate need to be informed of a particular signaling point/subsystem status change, independently of whether SCCP communication is in progress between the "concerned" entity and the affected entity with the status change.[18]

In some situations, the number of concerned subsystem or signaling points for a given subsystem may be zero. In this case, when that subsystem fails, or become unavailable, no broadcast of the subsystem prohibited message is performed. Instead, the response method is used to return the subsystem prohibited message. Similarly, no broadcast of the subsystem allowed message is performed for that given subsystem when it recovers. The response method is again used to return a subsystem allowed message in reply to a subsystem status test.

In the following procedures, the term "adjacent" is understood to mean logical adjacency. That is to say that node A is adjacent to node B if any SS7 path exists from A to B without a global title translator node in the path.

The signaling point prohibited, signaling point allowed, and signaling point congested procedures[19] -- specified in clauses 5.2.2, 5.2.3, and 5.2.4, respectively -- deal with the accessibility of a signaling point.

The subsystem prohibited and subsystem allowed procedures -- detailed in clauses 5.3.2 and 5.3.3, respectively -- deal with the accessibility of a subsystem.

An audit procedure to ensure that necessary subsystem management information is always available is specified in the subsystem status test procedure outlined in clause 5.3.4.

A subsystem may request to go out of service using the coordinated state change control procedure specified in clause 5.3.5

Local subsystems are informed of any related subsystem status by the local broadcast procedure specified in clause 5.3.6.

Concerned signaling points are informed of any related subsystem status by the broadcast procedure specified in clause 5.3.7.

Information regarding traffic patterns an SCCP user receives is provided by the traffic mix procedures outlined in clause 5.4.2.[15]

[15]The methods used in the calculation to determine traffic patterns are specified in clause 5.4.3.

[15]An audit procedure to ensure that necessary network-specific information is always available is specified in the subsystem routing status test procedure in clause 5.4.4.

---

[18] Further explicit definition of "concerned" subsystems or signaling points would be network/architecture/ application dependent.

[19] The congestion status of a signaling point may be used during translation to determine whether to route a received Class 0 message to the primary node/subsystem or to the backup node/subsystem if the option is selected to alternate route traffic because of signaling point congestion (defined on a per subsystem number basis). See clause 5.2.4.

5.2 Signaling Point Status Management

5.2.1 General

Signaling point status management updates translation and status based on the information of network failure, recovery, or congestion provided by the MTP-PAUSE indication, MTP-RESUME indication, or MTP-STATUS indication primitives. This allows alternative routing to replicate signaling points and/or replicate subsystems.

5.2.2 Signaling Point Prohibited

When SCCP management receives an MTP-PAUSE indication relating to a destination that becomes inaccessible, SCCP management:

1. Marks as "prohibited" the status of that signaling point.
2. Initiates a local broadcast (clause 5.3.6) of "signaling point inaccessible" information for that signaling point.
3. [20]Discontinues any SCCP status test for that signaling point.
4. [20]Marks as "prohibited" the status of that signaling point's SCCP.
5. [20]Initiates a local broadcast (clause 5.3.6) of "SCCP inaccessible" information for that signaling point's SCCP.
6. *If the indicated signaling point is a preferred node*, marks the translation as "translate to next preferred node" if that signaling point has a backup; or *if the indicated signaling point is a loadshare node*, marks the translation as 'translate to the remaining available loadshare nodes.' Otherwise, marks the affected node inaccessible.
7. Marks as "prohibited" the status of each subsystem at that signaling point.
8. Discontinues any subsystem status tests (clause 5.3.4) it may be conducting to any subsystems at that signaling point.
9. *If the signaling point is a preferred node*, marks the translation as "translate to next preferred subsystem" for each subsystem at that signaling point for which a backup subsystem exists; or *if the indicated signaling point is a loadshare node*, marks the translation as 'translate to the remaining available loadshare subsystems' for each subsystem at that signaling point for which a loadshare subsystem exists. Otherwise, marks the affected subsystems inaccessible.
10. Initiates a local broadcast (clause 5.3.6) of "User-out-of-service" information for each subsystem at that signaling point.
11. If the MTP-PAUSE pertains to the preferred node and traffic will be diverted to the next preferred node,[15] sends a Subsystem-Backup-Routing message regarding each replicated subsystem at that signaling point to SCCP management at the location of the corresponding next preferred subsystem. (This action is taken only if the node receiving the MTP-PAUSE is an "translator node" that is adjacent to the node at which the next preferred subsystem is located. For example, a signaling transfer point which learns that an adjacent database has failed sends a

[20] Flow Control procedures in clause 5.5 are optional.

Subsystem-Backup-Routing message to SCCP management for each next preferred subsystem at the next preferred node. If the signaling transfer point is not adjacent to the allowed next preferred subsystem, it does not send Subsystem-Backup-Routing messages.).

12. [15]Marks all local equipped duplicated subsystems backup routed from the failed signaling point, if the failed signaling point is an adjacent translator node.
13. [15]Initiates the traffic-mix information procedure (clause 5.4.2.1.1) to the local allowed users if the failed signaling point is an adjacent translator node.
14. [15]Stops all subsystem routing status tests for the failed signaling point (clause 5.4.4).

5.2.3 Signaling Point Allowed

When SCCP management receives an MTP-RESUME indication relating to a destination that becomes accessible, SCCP management:

1. Marks as "allowed" the status of that signaling point.
2. Resets the congestion level of the signaling point.
3. Initiates a local broadcast (clause 5.3.6) of "signaling point accessible" information for that signaling point.
4. [20]Discontinues any SCCP status test for that signaling point.
5. [20]Marks as "allowed" the status of the signaling point's SCCP.
6. [20]Initiates a local broadcast (clause 5.3.6) of "SCCP accessible" information for the signaling point's SCCP.
7. Marks the translation as: "translate to previously inaccessible higher priority node/subsystem," *if the signaling point is a replicated higher priority node*, or marks the translation as "translate to all available loadshare nodes," *if the signaling point is a loadshare node*.
8. Performs either action (a) or (b) for each subsystem:
    a. Except for the selected replicated subsystem (8b):
        i. Marks as "allowed" the status of each remote subsystem.
        ii. Initiates a local broadcast (clause 5.3.6) of "User-in-service" information for each subsystem at the signaling point.
        iii. Marks the translation as "translate to previously inaccessible higher priority subsystem" *for each replicated subsystem at the signaling point if the signaling point contains replicated higher priority subsystems*; or marks the translation as "translate to the all available loadshare subsystems" *for each loadshare subsystem at that signaling point*; or
    b. As a network provider option, for selected replicated subsystems (operating in either dominant or the loadshare mode), the subsystem status test procedure is initiated.
9. [15]Initiates, if the recovered signaling point is an adjacent translator node:
    a. The subsystem routing status test procedure (clause 5.4.4) for all local equipped duplicated subsystems.

b. The traffic-mix information procedure (clause 5.4.2.1.1) to the local allowed subsystems.

5.2.4 Signaling Point Congested

When SCCP management receives an MTP-STATUS indication relating to signaling network congestion to a signaling point, SCCP management:

1. Updates that signaling point status to reflect the congestion;
2. Initiates a local broadcast (clause 5.3.6) of "signaling point congested" information for that signaling point.

The congestion status of a signaling point may be used during translation to determine whether to route a received Class 0 message to the preferred node/subsystem or to the next preferred node/subsystem, if the option is selected to alternate route traffic because of signaling point congestion for the dominant mode (defined on a per subsystem number basis for replicated subsystems operating in the dominant mode). If the loadshare mode is in use, the congestion status of a signaling point may also be used during translation to determine if any of the loadshare node/subsystem should *not* receive a Class 0 message due to congestion.

5.2.5 SCCP Reaction to Local MTP Restart

When SCCP management receives an indication of the end of MTP Restart, SCCP management:

1. Resets the congestion level of the signaling points concerned by the restarting MTP.
2. Instructs the translation function to update the translation tables, taking into account the accessibility information given by the MTP indicating the end of MTP Restart.
3. Marks as "allowed" the status of the subsystems for each accessible point.
4. Initiates a local broadcast (clause 5.3.6) of "signaling point accessible."

5.3 Subsystem Status Management

5.3.1 General

Subsystem status management updates translation and status based on the information of failure, withdrawal, congestion, and recovery of subsystems. This allows alternative routing to next preferred subsystems or remaining available loadshare subsystems, if appropriate. Local users are informed of the status of their replicated subsystems.

5.3.2 Subsystem Prohibited

5.3.2.1 Receipt of Message for a Prohibited Subsystem

If SCCP routing control receives a message, whether originated locally or not, for a prohibited local subsystem, SCCP routing control invokes subsystem prohibited control. A Subsystem-Prohibited message is sent to the originating signaling point if the originating subsystem is not local (the OPC is a parameter in the MTP-TRANSFER indication primitive). The action, if any, to be taken, if the originating subsystem is local, is for further study.

5.3.2.2 Receipt of Subsystem-Prohibited Message or N-STATE Request Primitive or Local User Failed

Under one of the following conditions:

1. SCCP management receives a Subsystem-Prohibited message about a subsystem marked allowed;
2. An N-STATE request primitive with "User-out-of-service" information is invoked by a subsystem marked allowed; or
3. SCCP management detects that a local subsystem has failed;

Then SCCP management does the following:

1. If the Subsystem-Prohibited message pertains to the *preferred subsystem*, marks the translation as appropriate: "translate to next preferred subsystem" if the prohibited subsystem is replicated; or if the Subsystem-Prohibited message pertains to a *loadshare subsystem*, marks the translation as appropriate: "translate to remaining available loadshare subsystems";
2. Marks as "prohibited" the status of that subsystem;
3. Initiates a local broadcast (clause 5.3.6) of "User-out-of-service" information for the prohibited subsystem;
4. initiates the subsystem status test procedure (clause 5.3.4) if the prohibited subsystem is not local;
5. Forwards the information throughout the network by initiating a broadcast (clause 5.3.7) of Subsystem-Prohibited messages to concerned signaling points. The list of concerned signaling points should include, at a minimum, the mate subsystem. The list of concerned signaling points may also include replicates other than the mate subsystem, as well as other translator nodes with an immediate need to be informed of a particular change in status. The mate subsystem should be included in this list so that mates are aware of each other's status for coordinated state change purposes. The concerned signaling points for a particular subsystem are determined by the network provider;
6. If the Subsystem-Prohibited message pertains to the preferred subsystem[15], sends a Subsystem-Backup-Routing message to SCCP management at the node containing the next preferred subsystem if it has the translation capability and if the next preferred subsystem is located at an adjacent node;
7. Cancels "ignore subsystem status test" and the associated timer if they are in progress and if the newly prohibited subsystem resides at the local node;
8. Cancels "wait for grant" and the associated timer T(coord.chg) if they are in progress and if the newly prohibited subsystem resides at the local node.

5.3.3 Subsystem Allowed

Under one of the following conditions:

1. SCCP management receives a Subsystem-Allowed message about a subsystem marked prohibited; or
2. An N-STATE request primitive with "User-in-Service" information is invoked by a subsystem marked prohibited;

Then SCCP management does the following:

1. If the Subsystem-Allowed message pertains to a *higher priority subsystem*, marks the translation as appropriate: "translate to previously inaccessible higher priority subsystem" if the subsystem is replicated; or if the Subsystem-Allowed message pertains to a *loadshare subsystem*, marks the translation as appropriate: "translate to all available loadshare subsystems";
2. Marks as "allowed" the status of that subsystem;
3. Initiates a local broadcast (clause 5.3.6) of "User-in-service" information for the allowed subsystem;
4. Discontinues the subsystem status test relating to that subsystem if such a test was in progress;
5. Forwards the information throughout the network by initiating a broadcast (clause 5.3.7) of Subsystem-Allowed messages to concerned signaling points. The list of concerned signaling points should include, at a minimum, the mate subsystem. The list of concerned signaling points may also include replicates other than the mate subsystem, as well as other translator nodes with an immediate need to be informed of a particular change in status. The mate subsystem should be included in this list such that mates are aware of each other's status for coordinated state change purposes. It is unclear whether other replicates have an immediate need to be informed of changes in status. The concerned signaling points for a particular subsystem are determined by the network provider;
6. If the Subsystem-Allowed message pertains to a higher priority subsystem[15], sends -- if it has the translation capability -- a Subsystem-Normal-Routing message to SCCP management at the node containing the previously preferred subsystem (i.e., the node that previously received the Subsystem-Backup-Routing message), if that subsystem is located at an adjacent node;
7. [15]Initiates the traffic mix information procedure (clause 5.4.2.1.1), if the newly allowed subsystem resides at the local node.

5.3.4 Subsystem Status Test

5.3.4.1 General

The subsystem status test procedure is an audit procedure to verify the status of a subsystem marked prohibited. Use of the procedure is not required in nodes that only respond to received queries, e.g., some types of end node/databases.

5.3.4.2 Actions at the Initiating Node

A subsystem status test is initiated:

1. When a Subsystem-Prohibited message is received (clause 5.3.2.2); or
2. For selected replicated subsystems (a network provider option) when:
   a. An MTP-RESUME indication primitive for a previously inaccessible signaling point is received (clause 5.2.3), or;
   b. [20]A Subsystem-Allowed message for a previously unavailable remote SCCP is received (clause 5.5.3); or
   c. [20]A timer T(stat.info) expires for a previously unavailable remote SCCP is received (clause 5.5.3).

A subsystem status test associated with a failed subsystem is commenced by starting a timer T(stat.info) and marking a test in progress. No further actions are taken until the timer expires.

Upon expiration of the timer, a Subsystem-Status-Test message is sent to SCCP management at the node of the failed subsystem and the timer is reset.

The cycle continues until the test is terminated by another SCCP management function at that node. Termination of the test causes the timer and the test mark to be canceled.

5.3.4.3 Actions at the Receiving Node

When SCCP management receives a Subsystem-Status-Test message and there is no "ignore subsystem status test" in progress, it checks the status of the named subsystem. If the subsystem is allowed, a Subsystem-Allowed message is sent to SCCP management at the node conducting the test. If the subsystem is prohibited, no reply is sent.

5.3.5 Coordinated State Change

5.3.5.1 General

A replicated subsystem may be withdrawn from service without degrading the performance of the network by using the coordinated state change procedure described below when its replicate(s) are not local. The procedure, if any, to be specified in case the replicated subsystems are co-located, is for further study.

5.3.5.2 Actions at the Requesting Node

When a replicated subsystem wishes to go out of service, it invokes an N-COORD request primitive. SCCP management at that node sends a Subsystem-Out-of-Service-Request message to SCCP management at the node(s) containing the replicated subsystem(s), sets a timer T(coord.chg), and marks the subsystem as "waiting for grant." Arrival of all Subsystem-Out-of-Service-Grant message(s) at the requesting SCCP management causes the timer T(coord.chg) to be canceled, the "waiting for grant" state to be canceled, and a "granted" N-COORD confirmation primitive to be invoked to the requesting subsystem. Subsystem-Prohibited messages are broadcast (clause 5.3.7) to concerned signaling points.

In addition, an "ignore subsystem status test" timer is started and the requesting subsystem is marked as "ignore subsystem status test." Subsystem status tests are ignored until the "ignore subsystem status test" timer expires or the marked subsystem invokes an N-STATE request primitive with "User-out-of-service" information.

If no "waiting for grant" is associated with the subsystem named in the Subsystem-Out-of-Service-Grant message, the Subsystem-Out-of-Service-Grant message is discarded and no further action is taken.

If the timer associated with the subsystem waiting for the grant expires before all Subsystem-Out-of-Service-Grant message(s) are received, the "waiting for grant" is canceled and the request is explicitly denied by invoking a "denied" N-COORD confirmation primitive to the requesting subsystem.

5.3.5.3 Actions at the Requested Node

When the SCCP management at the node at which the replicated subsystem is located receives the Subsystem-Out-of-Service-Request message, it checks the status of local resources. If the SCCP has sufficient resources to assume the increased load, it invokes an N-COORD indication primitive to the local subsystem. If the SCCP does not have sufficient resources, no further action is taken[21].

If the local subsystem has sufficient resources to allow the requesting subsystem to go out of service, it informs SCCP management by invoking an N-COORD response primitive. A Subsystem-Out-of-Service-Grant message is sent to SCCP management at the requesting node. If the local subsystem does not have sufficient resources, no reply is returned[21].

5.3.6 Local Broadcast

5.3.6.1 General

The local broadcast procedure provides a mechanism to inform local allowed concerned subsystems of any related subsystem status or signaling point information received.

5.3.6.2 User-out-of-Service

A local broadcast of "User-out-of-service" information is initiated when:

1. A Subsystem-Prohibited message is received about a subsystem marked allowed (clause 5.3.2.2);
2. An N-STATE request primitive with "User-out-of-service" information is invoked by a subsystem marked allowed (clause 5.3.2.2);
3. A local subsystem failure is detected by SCCP management (clause 5.3.2.2);
4. An MTP-PAUSE indication primitive is received (clause 5.2.2); or

---

[21] The possibility of introducing an explicit Subsystem-Out-of-Service-Denial message containing additional information and associated primitive is for further study.

5. If SCCP Flow Control is used (clause 5.5), an MTP-STATUS indication primitive with "user part unavailable" information for the SCCP is received.

SCCP management then informs local allowed concerned SCCP subsystems about the subsystem status by invoking an N-STATE indication primitive with "User-out-of-service" information.

5.3.6.3 User-in-Service

A local broadcast of "subsystem-in-service" information is initiated when:

1. A Subsystem-Allowed message is received about a subsystem marked prohibited (clause 5.3.3);
2. An N-STATE request primitive with "User-in-service" information is invoked by a subsystem marked prohibited (clause 5.3.3);
3. If a subsystem is marked "allowed" on receipt of an MTP-RESUME indication (see clause 5.2.3);
4. An indication of the end of MTP Restart is received (see clause 5.2.5); or
5. If SCCP Flow Control is used (see clause 5.5), then if a subsystem is marked "allowed" when:
   a. A Subsystem-Allowed message is received with SSN=1 about a remote SCCP marked prohibited; or
   b. Timer T(stat.info) expires but an MTP-STATUS primitive indicating remote SCCP unavailability has not been received since the timer is started or restarted.

SCCP management then informs local allowed concerned SCCP subsystems, except the newly allowed one, about the subsystem status by invoking an N-STATE indication primitive with "User-in-service" information.

5.3.6.4 Signaling Point Inaccessible

A local broadcast of "signaling point inaccessible" information is initiated when an MTP-PAUSE primitive is received; SCCP management then informs local allowed concerned SCCP subsystems about the signaling point status by invoking an N-PCSTATE indication primitive with "signaling point inaccessible" information.

5.3.6.5 Signaling Point Accessible

A local broadcast of "signaling point accessible" information is initiated when an MTP-RESUME primitive is received. SCCP management then informs local allowed concerned SCCP subsystems about the signaling point status by invoking an N-PCSTATE indication primitive with "signaling point accessible" information.

5.3.6.6 Signaling Point Congested

A local broadcast of "signaling point congested" information is initiated when an MTP-STATUS primitive is received. SCCP management then informs local allowed concerned SCCP subsystems about the signaling point status by invoking an N-PCSTATE indication primitive with "signaling point congested (level)" information.

5.3.6.7 SCCP Inaccessible[20]

A local broadcast of "SCCP inaccessible" information is initiated when an MTP-PAUSE primitive is received or an MTP-STATUS primitive (with "user part unavailable" information for the SCCP) is received. SCCP management then informs local allowed concerned SCCP subsystems about the SCCP status by invoking an N-PCSTATE indication primitive with "SCCP inaccessible" information.

5.3.6.8 SCCP Accessible[20]

A local broadcast of "SCCP accessible" information is initiated when an MTP-RESUME primitive is received or when:

1. A Subsystem-Allowed message is received with SSN=1 about a remote SCCP marked prohibited, or;
2. Timer T(stat.info) expires, but an MTP-STATUS primitive indicating remote SCCP unavailability has not been received since the timer was started or restarted.

SCCP management then informs local allowed concerned SCCP subsystems about the signaling point status by invoking an N-PCSTATE indication primitive with "SCCP accessible" information.

5.3.7 Broadcast

5.3.7.1 General

The broadcast procedure provides a mechanism that may be used to inform concerned signaling points of any related subsystem status change at local or adjacent signaling points.

5.3.7.2 Subsystem Prohibited

A broadcast of Subsystem-Prohibited messages is initiated when:

1. A Subsystem-Prohibited message is received about a subsystem presently marked allowed (clause 5.3.2.2), and the affected point code identified in the SSP message is the same as that of the informer signaling point;
2. An N-STATE request primitive with "User-out-of-service" information is invoked by a subsystem marked allowed (clause 5.3.2.2);
3. A local subsystem failure is detected by SCCP management (clause 5.3.2.2); or
4. A Subsystem-Out-of-Service-Grant message arrives for a subsystem marked "waiting for grant" (clause 5.3.5.2).

This broadcast permits SCCP management to inform all concerned signaling points, except the informer signaling point, about the subsystem status by Subsystem-Prohibited messages. SCCP management does not broadcast if the point code of the prohibited subsystem is different from that of the informer signaling point which originates the Subsystem-Prohibited message.

5.3.7.3 Subsystem Allowed

A broadcast of Subsystem-Allowed messages is initiated when:

1. A Subsystem-Allowed message is received about a subsystem presently marked prohibited (clause 5.3.3), and the affected point code identified in the SSA message is the same as that of the informer signaling point, or
2. An N-STATE request primitive with "User-in-service" information is invoked by a subsystem marked prohibited (clause 5.3.3).

This broadcast permits SCCP management to inform all concerned signaling points, except the informer signaling point, about the subsystem status by Subsystem-Allowed messages. SCCP management does not broadcast if the point code of the allowed subsystem is different from that of the informer signaling point which originates the Subsystem-Allowed message.

5.4 Traffic Information Management (Optional)

Traffic information management procedures apply only to a replicated subsystem with a single backup (primary/secondary node/subsystem configuration).

NOTE - Traffic information management procedures are architecture dependent and therefore require further study for application to different network architectures.

5.4.1 General

Traffic information management procedures provide a mechanism for informing SCCP users of received traffic patterns as described in ATIS-1000112.1.

5.4.2 Traffic Mix Procedures

There is one generic traffic mix information procedure to inform local users of the local consequences of:

1. Signaling point inaccessibility;
2. Signaling point accessibility;
3. Backup routing to subsystem; or
4. Normal routing to subsystem.

The traffic pattern is determined by analyzing the subsystem multiplicity indicator, the status of adjacent translator nodes, and the routing flags. A routing flag, associated with a subsystem, is used to indicate the type of traffic (normal or backup) the subsystem is receiving from its adjacent translator node.

The analysis is performed on the basis of node category. Thus, there is one specific traffic-mix information procedure for each node category. The methods used to determine the traffic pattern are specified in clause 5.4.3.

Node category serves to differentiate the position and function of a node in the network. "End-node/database" and "intermediate-node/translator" are two examples. Traffic mix procedures are currently provided only at "end-node/databases."

5.4.2.1 End-Node/Database

5.4.2.1.1 Traffic-Mix Information

SCCP management may invoke an N-TRAFFIC indication primitive with "Traffic-mix" information to each local concerned user, when one of the following occurs:

1. The MTP invokes an MTP-PAUSE indication primitive;
2. The MTP invokes an MTP-RESUME indication primitive;
3. A Subsystem-Backup-Routing message is received by SCCP management;
4. A Subsystem-Normal-Routing message is received by SCCP management; or
5. An N-STATE request primitive with "User-in-Service" information is invoked by a subsystem marked prohibited.

5.4.2.1.2 Subsystem Backup Routing

Upon receipt of a Subsystem-Backup-Routing message from an adjacent signaling point and if the affected subsystem in the message is replicated locally, SCCP management:

1. Marks the routing flag associated with:
    a. The signaling transfer point from which the Subsystem-Backup-Routing message was received; and
    b. The local replicate subsystem of the subsystem to which the message refers to "backup."
2. Initiates a subsystem routing status test (clause 5.4.4); and
3. Initiates a traffic-mix information procedure (clause 5.4.2.1.1) to the local replicate subsystem if it's allowed.

5.4.2.1.3 Subsystem Normal Routing

Upon receipt of a Subsystem-Normal-Routing message from an adjacent signaling point and if the affected subsystem in the message is replicated locally, SCCP management:

1. Marks the routing flag associated with:

a. The signaling transfer point from which the Subsystem-Normal-Routing message was received; and

b. The local replicate subsystem of the subsystem to which the message refers to "normal."

2. Stops the subsystem routing status test (clause 5.4.4); and

3. Initiates a traffic-mix information procedure (clause 5.4.2.1.1) to the local replicate subsystem, if it's allowed.

5.4.3 Calculation of Traffic-Mix Information

5.4.3.1 General

The quasi-associated network (see ATIS-1000111.5, Annexes 1 and 2) uses one piece of additional information called the routing flag. The routing flag provides additional network connectivity information. Two network-specific messages, Subsystem-Backup-Routing and Subsystem-Normal-Routing, allow the value (i.e., "backup" or "normal") of the routing flag to be determined.

Subsystem routing status messages are sent only by translator nodes adjacent to the end node at which a subsystem has become recovered or prohibited. When a subsystem becomes inaccessible, and SCCP management marks a subsystem "translate to next preferred subsystem," a Subsystem-Backup-Routing message is sent to the SCCP management associated with the next preferred subsystem. When a higher priority subsystem recovers, and SCCP management marks a subsystem "translate to previously inaccessible higher priority subsystem," a Subsystem-Normal-Routing message is transferred to the SCCP management associated with the previously preferred subsystem.

NOTE - The calculation of the traffic-mix information is architecture dependent rather than network dependent.

5.4.3.2 End-Node/Database

The method of determining the traffic pattern received by a local user at an "end-node/database" is summarized in Figure 18/ATIS-1000112.4. The possible failure combinations upon which this method is based are shown in Figure 19/ATIS-1000112.4.

Traffic-mix information is currently provided only at "end-node/databases."

5.4.4 Subsystem Routing Status Test

5.4.4.1 General

The subsystem routing status test procedure is an audit procedure to verify the routing status of a replicated subsystem marked back-up routed.

5.4.4.2 Actions at the Initiating Node

A subsystem routing status test is initiated when:

1. A Subsystem-Backup-Routing message is received (clause 5.4.2.1.2); or

2. An MTP-RESUME indication primitive for a previously inaccessible adjacent translator node is invoked (clause 5.2.3).

A subsystem routing status test associated with a subsystem is commenced by starting a timer T(rtg.stat.info) and marking a test in progress. No further actions are taken until the timer expires.

Upon expiration of the timer, a Subsystem-Routing-Status-Test message is sent to SCCP management at the node from which the Subsystem-Backup-Routing message was received, and the timer T(rtg.stat.info) is restarted.

The cycle continues until the test is terminated by another SCCP management function at that node. Termination of the test causes the timer and the test marked to be canceled.

5.4.4.3 Actions at the Receiving Node

When SCCP management receives an SRT message, it checks the status of the routing flags. If the routing is normal, a Subsystem-Normal-Routing message is sent to SCCP management at the node conducting the test. If there is backup routing, no reply is sent.

5.5 SCCP Flow Control (Optional)

5.5.1 General

SCCP Flow control supports the suspension and resumption of SCCP traffic to a remote signaling point where the SCCP functionality has recently failed or recovered.

5.5.2 SCCP Prohibited Control.

When SCCP management receives an MTP-STATUS primitive indicating that the status of a remote SCCP is "inaccessible," "unequipped," or "unknown," SCCP management:

1. If the status indicated for the remote SCCP is "inaccessible" or "unknown," initiates the SCCP Status Test (clause 5.5.4); and
2. Performs actions (4) through (14) described in clause 5.2.2, Signaling Point Prohibited Control.

5.5.3 SCCP Allowed Control

When, for a remote SCCP marked "prohibited":

a) A Subsystem-Allowed message with SSN=1 is received; or

b) Timer T(stat.info) expires, but an MTP-STATUS primitive indicating remote SCCP unavailability has not been received since the timer was started or restarted;

Then SCCP management:

1. Performs actions (4) through (9) described in clause 5.2.3 terminates, if Subsystem-Allowed message received; or

2. Performs actions (5) through (9) described in clause 5.2.3, if time T(stat.info) expires.

5.5.4 SCCP Status Test

An SCCP status test is initiated when MTP-STATUS indication for an inaccessible or unknown SCCP is received (clause 5.5.2).

An SCCP status test associated with an inaccessible or unknown SCCP is commenced by sending a Subsystem-Status-Test message (with the subsystem number set to one to indicate an SCCP status test) to the remote SCCP and starting a timer T(stat.info). The timer is reset if another SST initiation request is received for the inaccessible or unknown SCCP. This cycle continues until the test is terminated by another SCCP management function at that node. Termination of the test causes the timer to be canceled.

The expiration of the timer T(stat.info) for an inaccessible or unknown SCCP is handled by the SCCP Allowed Control procedure (clause 5.5.3).

When SCCP management receives a Subsystem-Status-Test message (SSN=1), a Subsystem-Allowed (SSN=1) message is sent to SCCP management at the node conducting the test.

5.6 SCCP Restart.

On a signaling point restart, an indication is given to the SCCP by the MTP about the signaling points which are accessible after the restart actions. For each accessible, concerned signaling point, all subsystems are marked allowed. If SCCP Flow Control is used with the signaling point, the status of its SCCP is also marked "allowed." The response method is used to determine the status of subsystems and the SCCP in those signaling points.

At the restarted signaling point, the status of its own subsystems are not broadcast to concerned signaling points. In this case, the response method is used to inform other nodes attempting to access prohibited subsystems at the restarted signaling point.

The actions to be taken in case of local MTP restart are described in clause 5.2.5.

6 STATE TRANSITION DIAGRAMS

6.1 General

This clause contains the description of the signaling network functions described in clauses 2 through 5 according to the CCITT Specification and Description Language.

A set of diagrams is provided for each of the following major functions:

1. SCCP routing control (SCRC), described in clause 2;
2. SCCP connection oriented control (SCOC), described in clause 3;
3. SCCP connectionless control (SCLC), described in clause 4; and

4. SCCP management (SCMG) described in clause 5.

For each major function, Figure 1/ATIS-1000112.4 illustrates a subdivision into functional specification blocks, showing their functional interactions as well as the interactions with the other major functions. In each case, this is followed by figures showing state transition diagrams for each of the functional specification blocks.

The detailed functional breakdown shown in the following diagrams is intended to illustrate a reference model, and to assist interpretation of the text in the earlier section. The state transition diagrams are intended to show precisely the behavior of the signaling system under normal and abnormal conditions as viewed from a remote location. It must be emphasized that the functional partitioning shown in the following diagrams is used only to facilitate understanding of the system behavior, and is not intended to specify the functional partitioning to be adopted in a practical implementation of the signaling system.

6.2 Drafting Conventions

Each major function is designated by its acronym (e.g., SCMG = SCCP management).

Each functional block is designated by an acronym which identifies it (e.g., SSAC = Subsystem allowed control).

External inputs and outputs are used for interactions between different functional blocks. Included within each input and output symbol in the state transition diagrams are acronyms which identify the functions which are the source and destination of the message, for example:

SSAC → SSTC indicates that the message is sent within a functional level
from: subsystem allowed control
to: subsystems status test control

Internal inputs and outputs are only used to indicate control of time-outs.

6.3 SCCP Routing

Figure 2/ATIS-1000112.4 shows the detailed functional specification of the SCCP Routing (SCRC) in a state transition diagram.

6.4 SCCP Connection-Oriented Control

Figures 2A/ATIS-1000112.4 to 2K/ATIS-1000112.4 show the detailed functional specification of the SCCP Connection - Oriented Control (SCOC) and Connection-Oriented Restart Control (SCOR) procedures in state transition diagrams as follows:

- Figure 2A/ATIS-1000112.4 Connection establishment and release procedures at originating node (Sheet 1, 2 and 3, connection establishment and sheet 4, connection release.)
- Figure 2B/ATIS-1000112.4 Connection establishment and release procedures at destination node (Sheet 1, connection establishment and sheet 2, connection release.)

- Figure 2C/ATIS-1000112.4 Data transfer at originating and destination nodes
- Figure 2D/ATIS-1000112.4 Expedited data transfer at originating and destination nodes
- Figure 2E/ATIS-1000112.4 Reset at originating and destination node
- Figure 2F/ATIS-1000112.4 Connection establishment and release procedures at intermediate node (Sheets 1, 2 and 3, connection establishment and sheet 4, connection release.)
- Figure 2G/ATIS-1000112.4 Data transfer procedures at intermediate node
- Figure 2H/ATIS-1000112.4 Expedited data transfer procedures at intermediate node
- Figure 2I/ATIS-1000112.4 Reset procedures at intermediate node
- Figure 2J/ATIS-1000112.4 Restart procedure at the recovered node
- Figure 2K/ATIS-1000112.4 Restart Control for SCCP Connection-Oriented Control

6.5 SCCP Connectionless Control

Figure 3/ATIS-1000112.4 shows the detailed functional specification of the SCCP Connectionless Control (SCLC) in a state transition diagram.

6.6 SCCP Management

Figure 4/ATIS-1000112.4 shows a subdivision of the SCCP Management function into smaller functional specification blocks, and also shows the functional interactions between them. Each of these functional specification blocks is described in detail in a state transition diagram as follows:

- Figure 5/ATIS-1000112.4 Signaling Point Prohibited Control (SPPC)
- Figure 6/ATIS-1000112.4 Signaling Point Allowed Control (SPAC)
- Figure 7/ATIS-1000112.4 Signaling Point Congested Control (SPCC)
- Figure 8/ATIS-1000112.4 Subsystem Prohibited Control (SSPC)
- Figure 9/ATIS-1000112.4 Subsystem Allowed Control (SSAC)
- Figure 10/ATIS-1000112.4 Subsystem Status Test Control (SSTC)
- Figure 11/ATIS-1000112.4 Coordinated State Change Control (CSCC)
- Figure 12/ATIS-1000112.4 Local Broadcast (LBCS)
- Figure 13/ATIS-1000112.4 Broadcast (BCST)
- Figure 14/ATIS-1000112.4[15] Traffic-Mix Information (TFMI)
- Figure 15/ATIS-1000112.4[15] Subsystem Backup Routing Control (SBRC)
- Figure 16/ATIS-1000112.4[15] Subsystem Normal Routing Control (SNRC)
- Figure 17/ATIS-1000112.4[15] Subsystem Routing Status Test Control (SRST)

6.7 Architecture Dependent Functions

Figure 18/ATIS-1000112.4 shows the determination of traffic patterns at "end-node/databases." Figure 19/ATIS-1000112.4 shows possible link failure combinations.

6.8 Abbreviations and Timers

Abbreviations and timers used in Figures 1/ATIS-1000112.4 through 19/ATIS-1000112.4 are listed below:

AP	All-primary
APAB	All-primary/All-backup
APNB	All-primary/No-backup
APSB	All-primary/Some-backup
BCST	Broadcast
CL	Connectionless
CO	Connection-oriented
CSCC	Coordinated State Change Control
DPC	Destination Point Code
GT	Global Title
LBCS	Local Broadcast
MTP	Message Transfer Part
NP	No-primary
NPNB	No-primary/No-backup
PC	Point Code
SBR	Subsystem-Backup-Routing
SBRC	Subsystem Backup Routing Control
SCLC	SCCP Connectionless Control
SCMG	SCCP Management
SCOC	SCCP Connection-oriented Control
SCRC	SCCP Routing Control
SLS	Signaling Link Selection
SNR	Subsystem-Normal-Routing
SNRC	Subsystem Normal Routing Control
SOG	Subsystem-Out-of-Service-Grant
SOR	Subsystem-Out-of-Service-Request
SP	Some-primary
SPAC	Signaling Point Allowed Control
SPCC	Signaling Point Congested Control
SPNB	Some-primary/No-backup
SPPC	Signaling Point Prohibited Control
SPSB	Some-primary/Some-backup
SRT	Subsystem-Routing-Status-Test
SRTC	Subsystem Routing Status Test Control

SSA	Subsystem-Allowed
SSAC	Subsystem Allowed Control
SSN	Subsystem Number
SSP	Subsystem-Prohibited
SSPC	Subsystem Prohibited Control
SST	Subsystem-Status-Test
SSTC	Subsystem Status Test Control
UIS	User-in-Service
UOD	User-Out-of-Service-Deny
UOG	User-Out-of-Service-Grant
UOR	User-Out-of-Service-Request
UOS	User-Out-of-Service

Timers

T(stat.info)	Delay between requests for subsystem status information with recommended value of 30 seconds.
T(coord.chg)	Waiting for grant for subsystem to go out of service with recommended value of 30 seconds.
T(ignore.SST)	Delay for subsystem between receiving grant to go out of service and actually going out of service with recommended value of 30 seconds.
T(rtg.stat.info)	Delay between requests for subsystem routing status information with recommended value of 30 seconds.
T(fr)	Waiting to reuse Segmentation Local Reference number; value implementation dependent.
T(reassembly)	Waiting to receive all the segments of the remaining segments of a segmented message after receiving the first segment; provisional range of 5 to 20 seconds.
T(conn.est)	Waiting to receive a CC message; provisional range of 1 to 2 minutes.
T(rel)	Waiting to receive a RLC message; provisional range of 10 to 20 seconds.
T(reset)	Waiting to release temporary connection section or alert maintenance function after an RSR message is sent; provisional range of 10 to 20 seconds.
T(ias)	Delay to send a message on a connection section; provisional range of 5 to 10 minutes.
T(iar)	Waiting to receive a message on a connection section; provisional range of 11 to 21 minutes.
T(guard)	Waiting to resume normal procedures for temporary signaling connections during the restart procedure (see clause 3.8); provisional range of 23 to 25 minutes.
T(int)	Waiting for RLC message; or to release connection resources, freeze the Local Reference Number and alert a maintenance function after the initial T(rel) expiry; up to 1 minute.
T(repeat_rel)	Waiting for RLC message; or to repeat sending RLSD message after the initial T(rel) expiry; provisional range of 10 to 20 sec.

Note that the standard numbering has changed in this version of ATIS-1000111, ATIS-1000112, and ATIS-1000113. These standards were formerly numbered as T1.111, T1.112, and T1.113 respectively. The associated chapter numbering has not been modified.

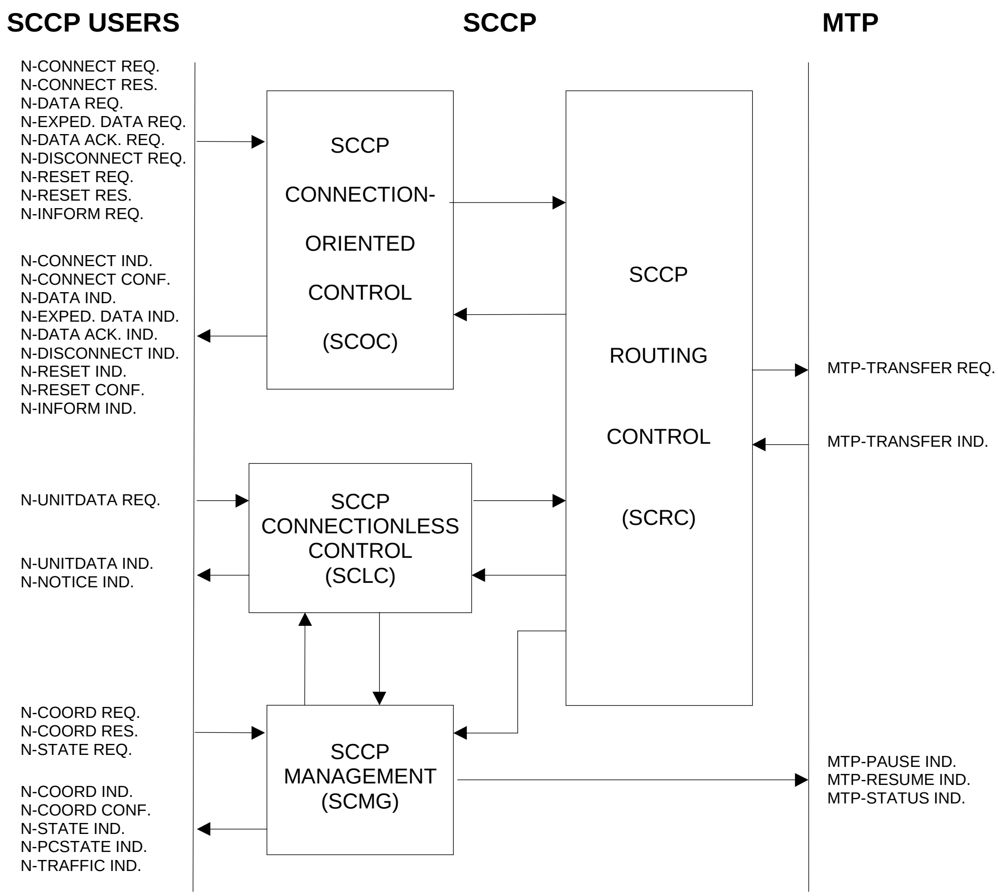


Figure 1/ATIS-1000112.4 - SCCP Overview

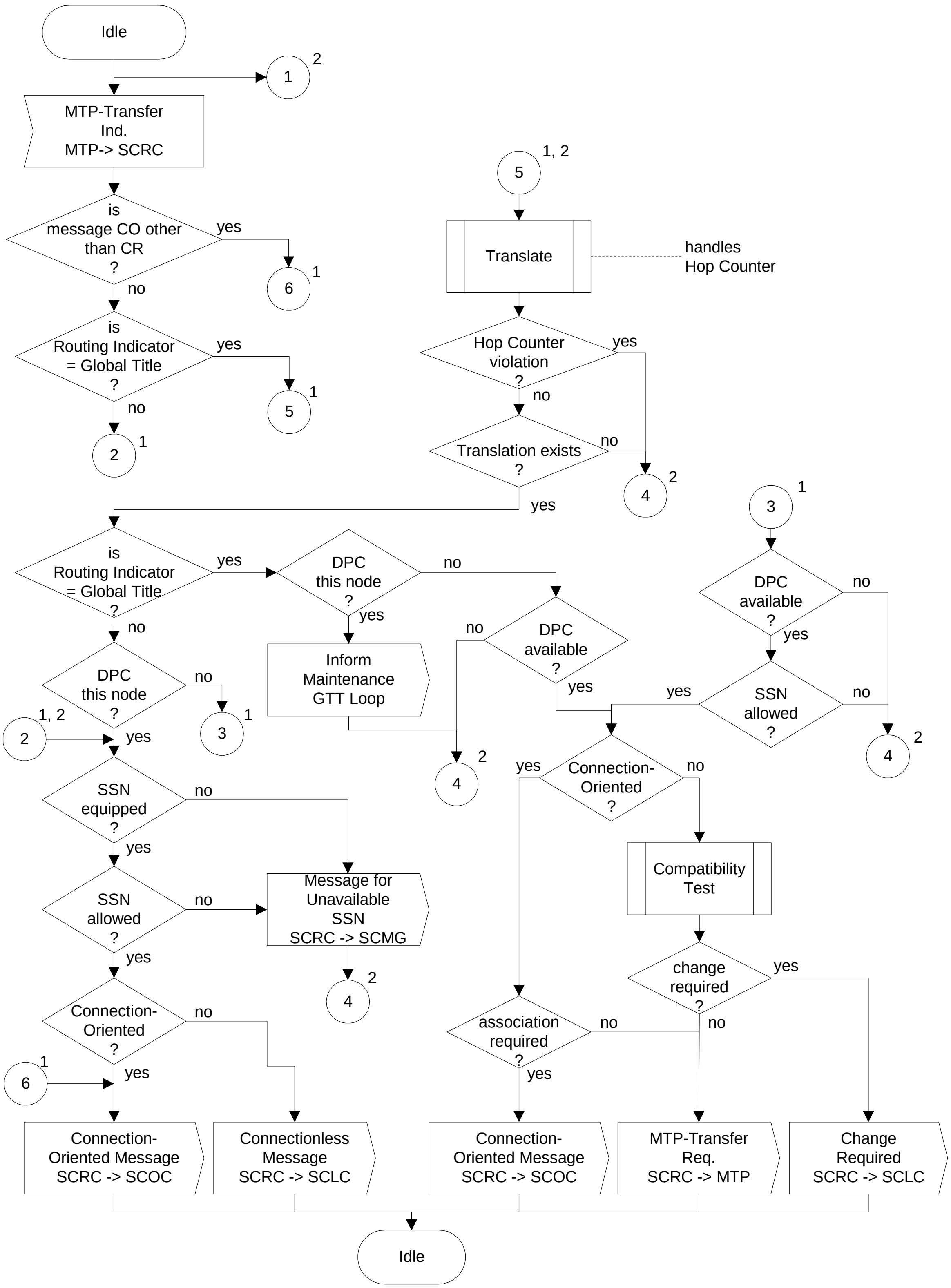


Figure 2/ATIS-1000112.4 -SCCP Routing Control Procedures (SCRC) (Sheet 1 of 2)

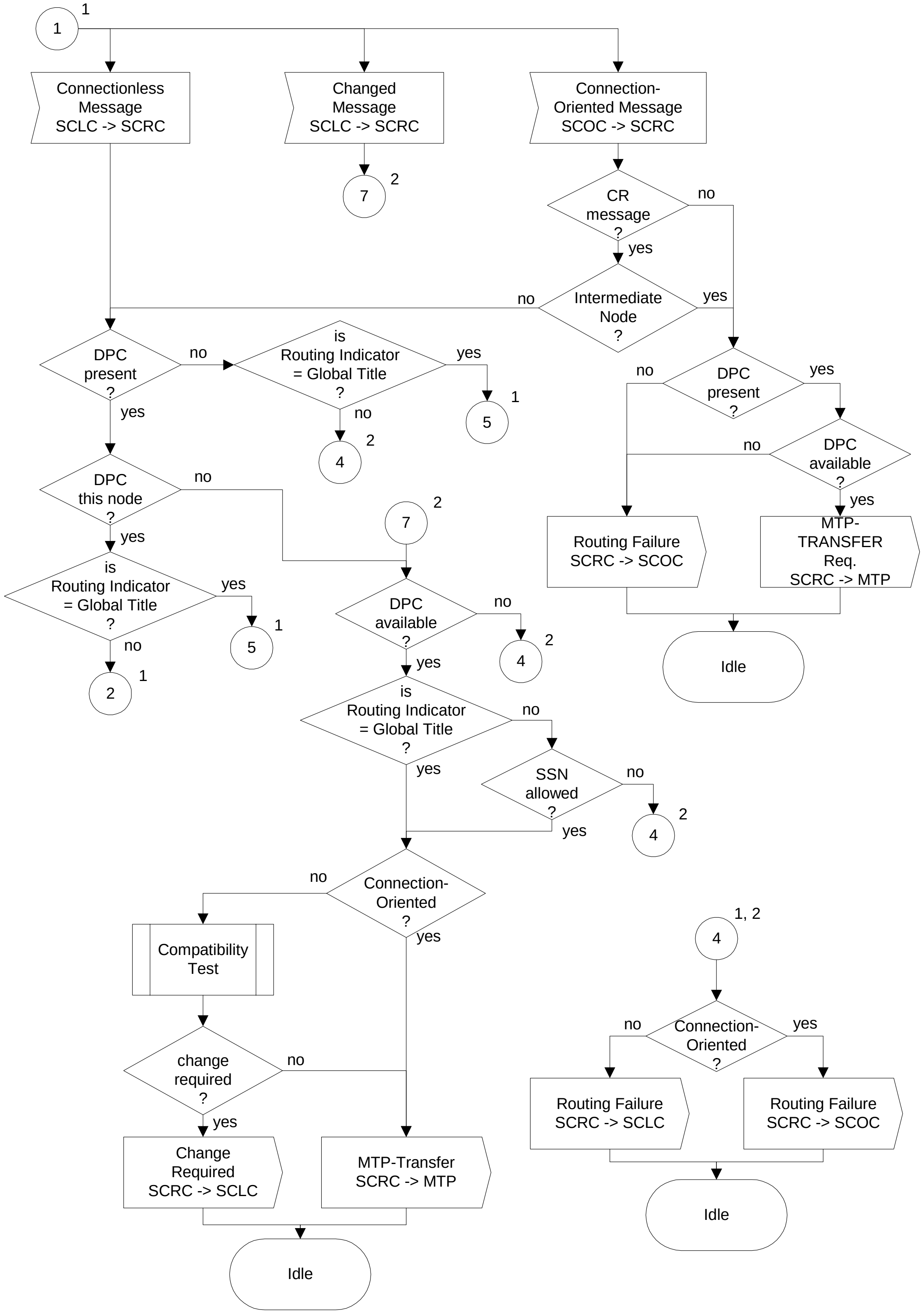


Figure 2/ATIS-1000112.4 - SCCP Routing Control Procedures (SCRC) (Sheet 2 of 2)

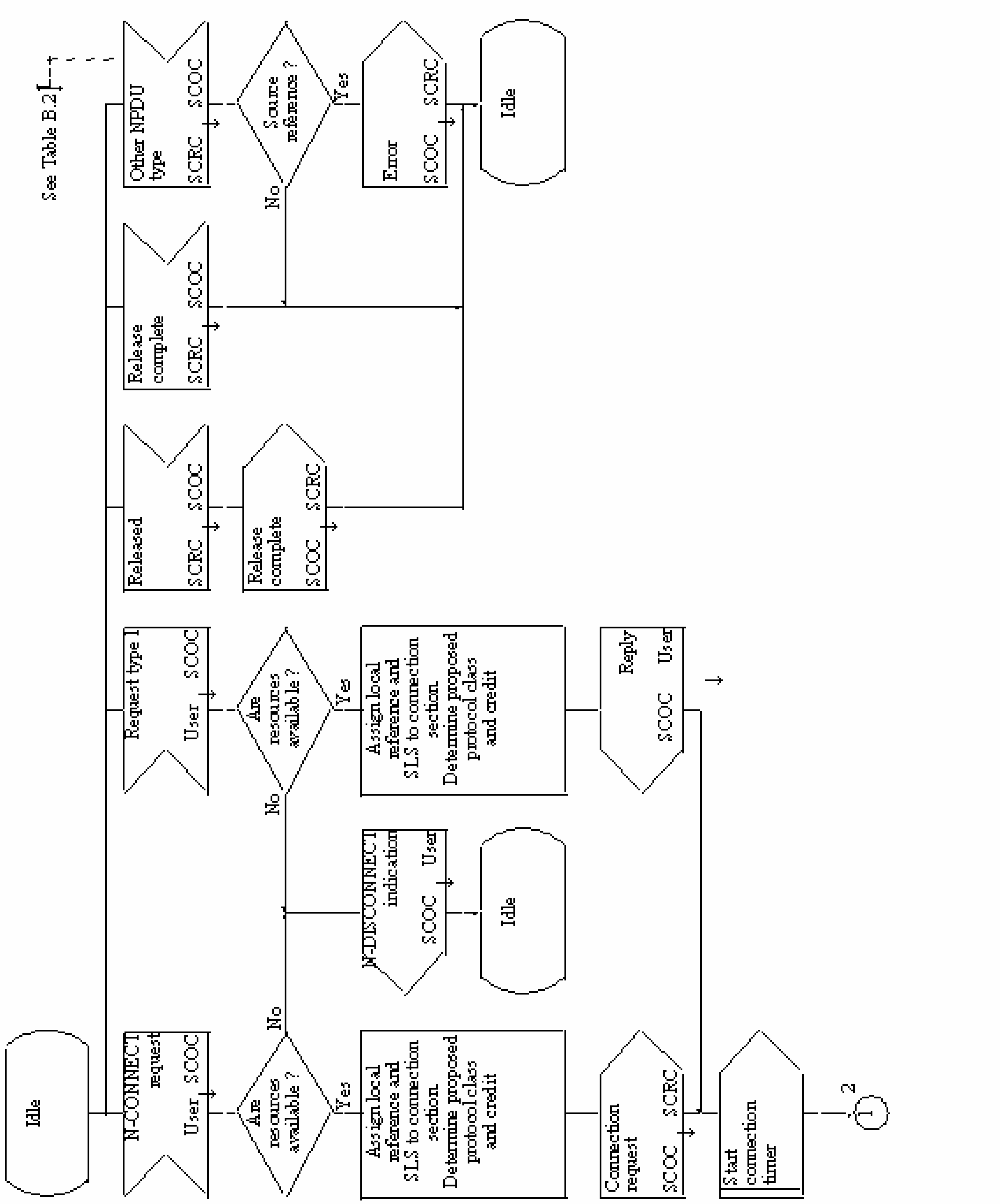


Figure 2A/ATIS-1000112.4 - SCOC, Connection establishment procedures at originating node (Sheet 1 of 7)

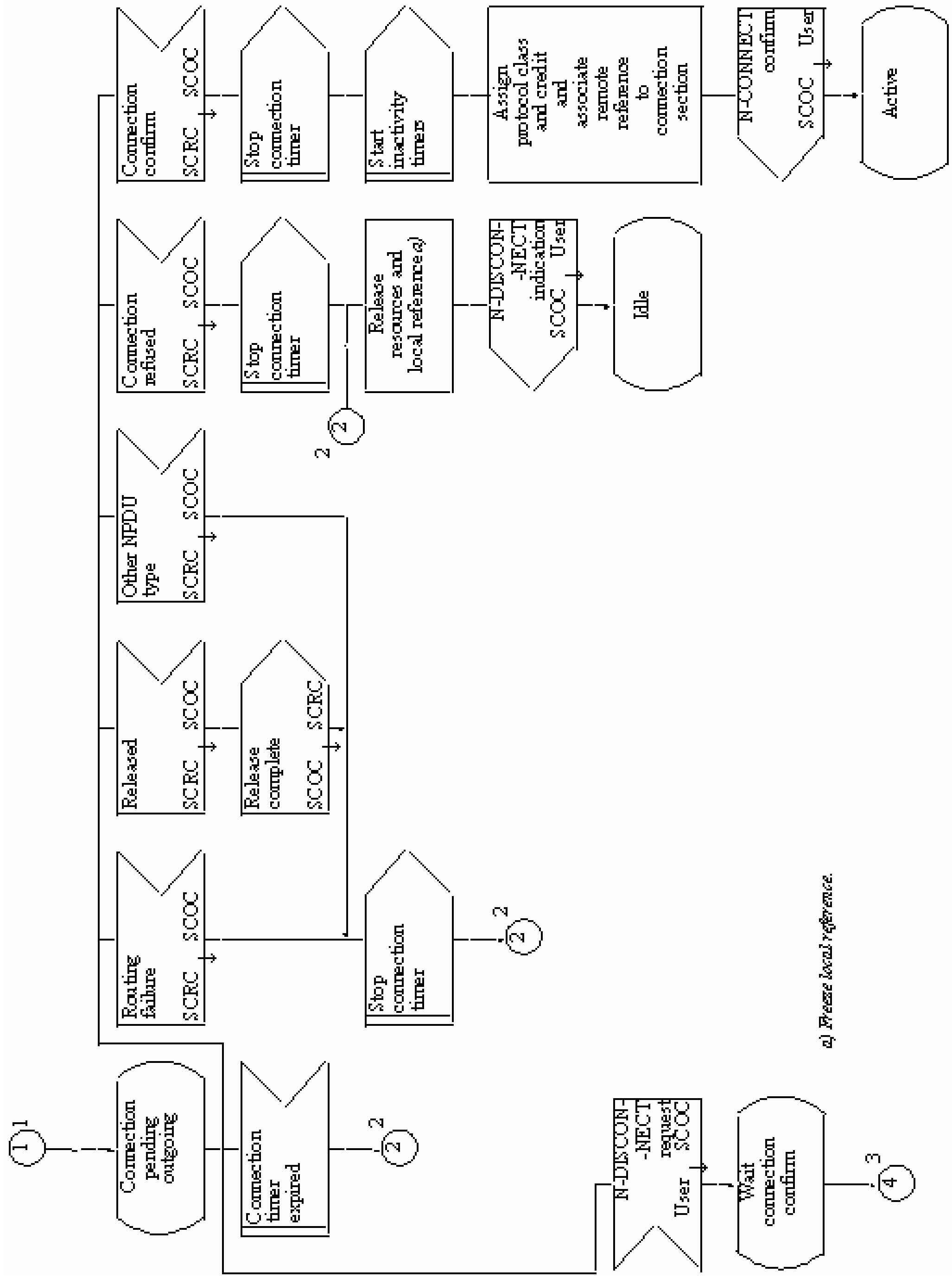


Figure 2A/ATIS-1000112.4 - SCOC, Connection establishment procedures at originating node (Sheet 2 of 7)

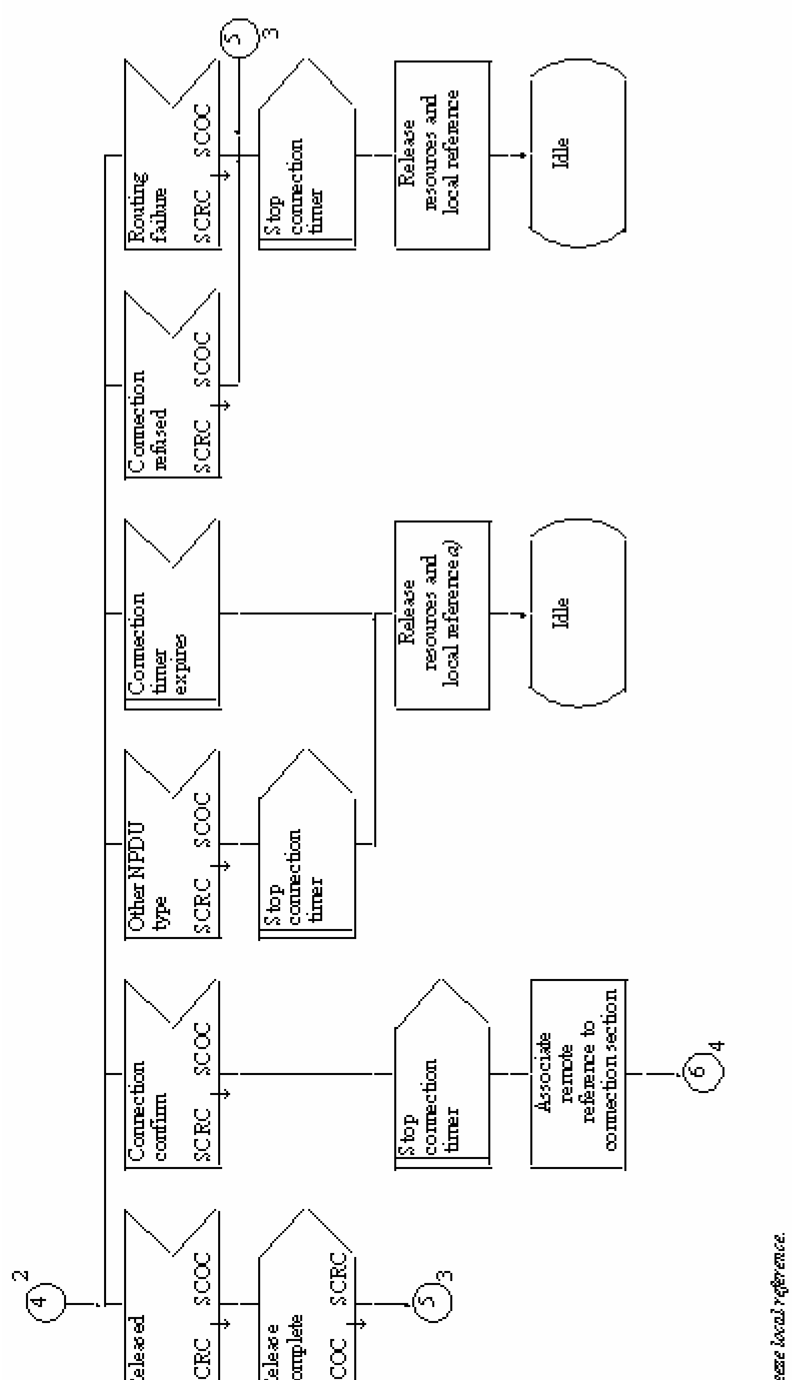


Figure 2A/ATIS-1000112.4 - SCOC, Connection establishment procedures at originating node (Sheet 3 of 7)

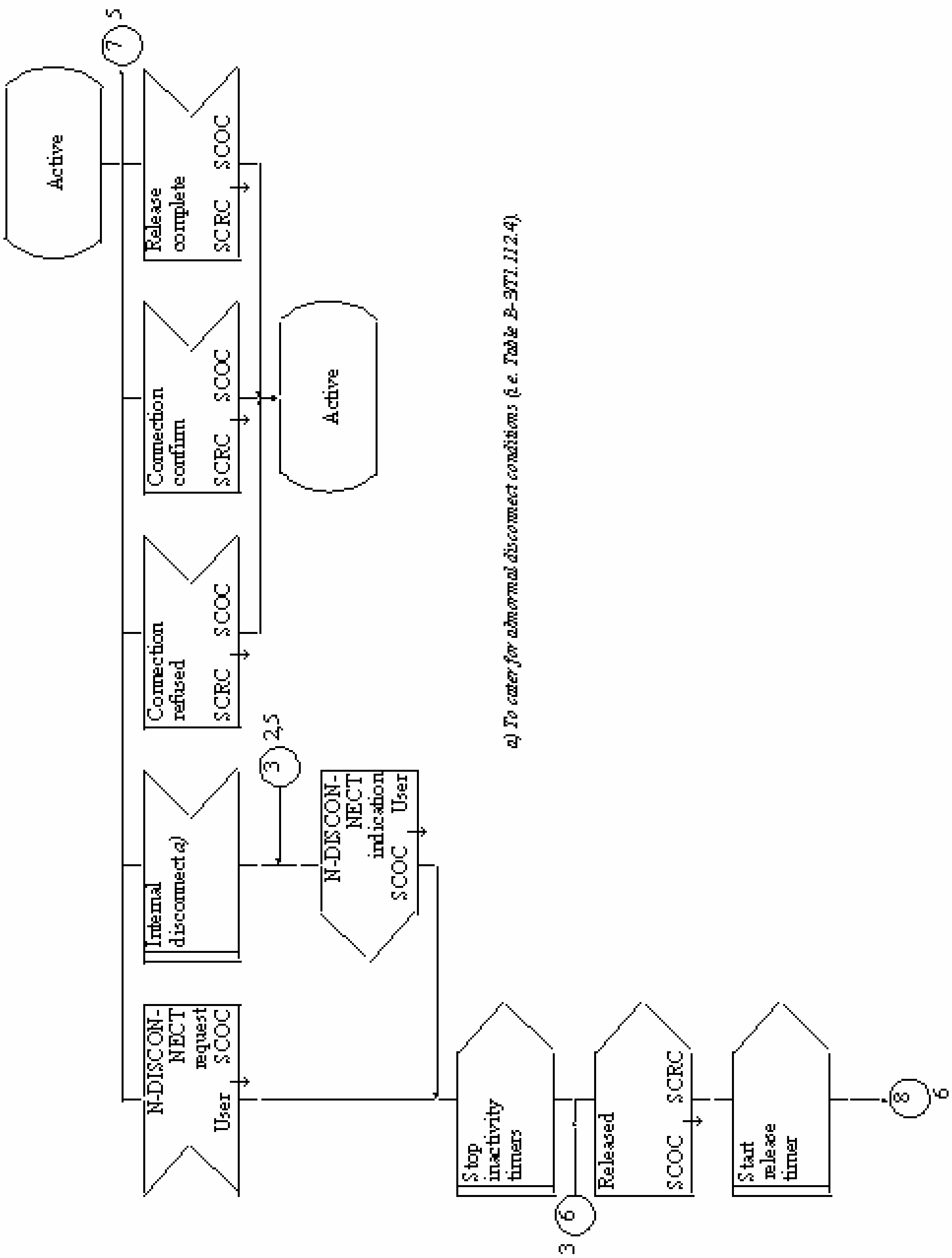


Figure 2A/ATIS-1000112.4 - SCOC, Connection establishment procedures at originating node (Sheet 4 of 7)

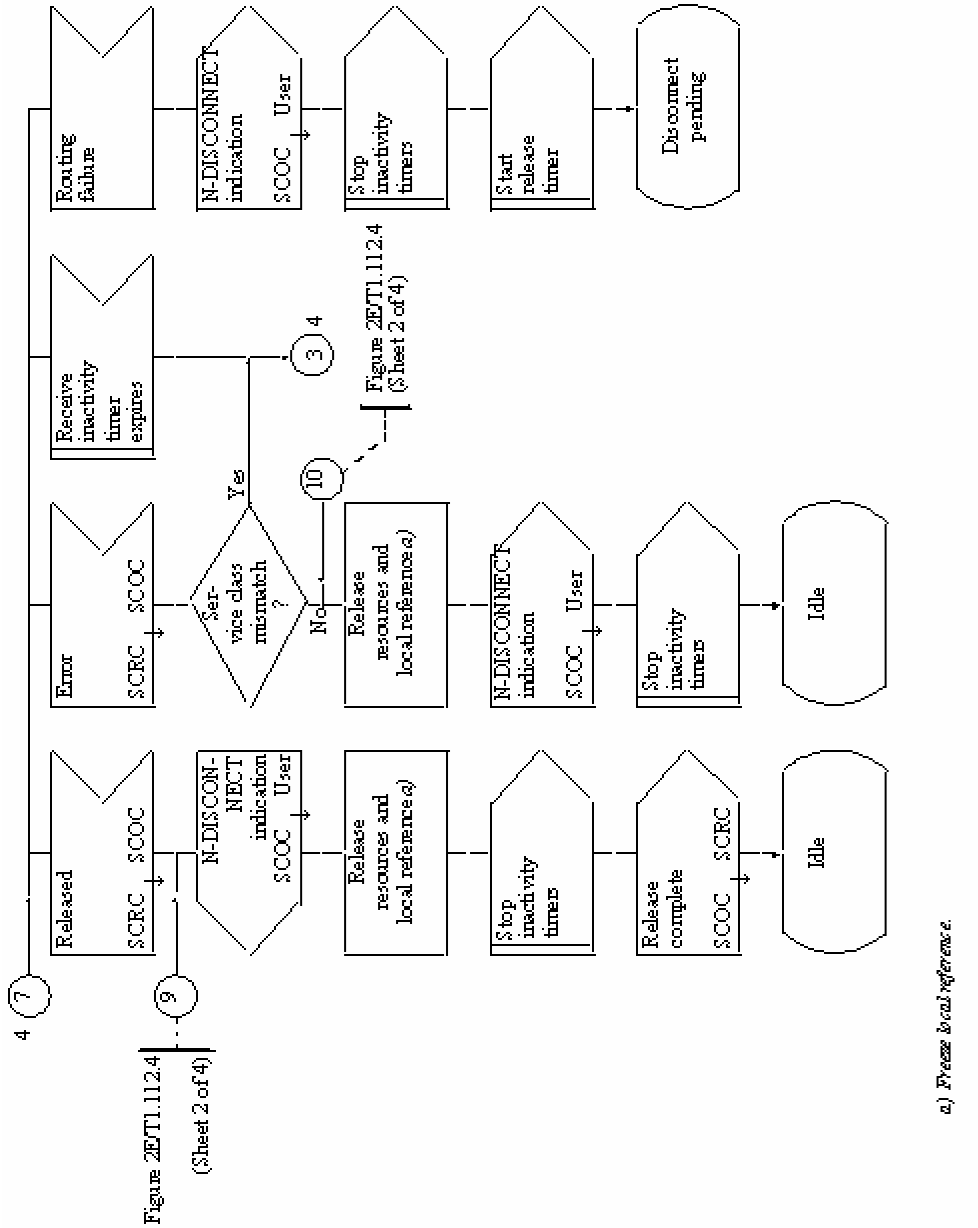


Figure 2A/ATIS-1000112.4 - SCOC, Connection establishment procedures at originating node (Sheet 5 of 7)

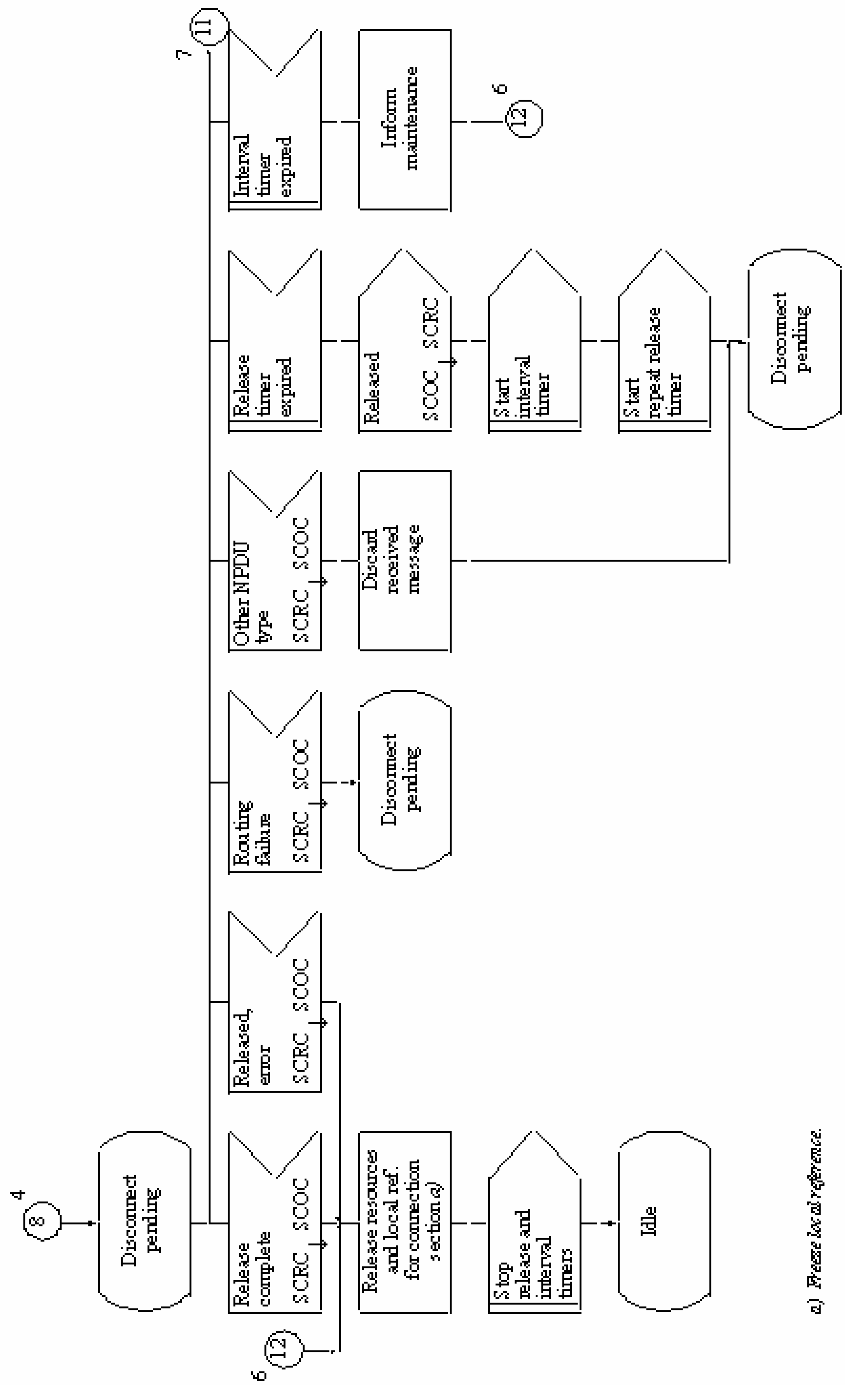


Figure 2A/ATIS-1000112.4 - SCOC, Connection establishment procedures at originating node (Sheet 6 of 7)

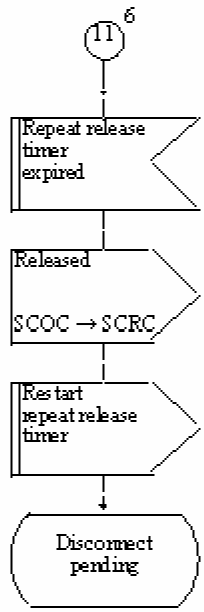


Figure 2A/ATIS-1000112.4 - SCOC, Connection establishment procedures at originating node (Sheet 7 of 7)

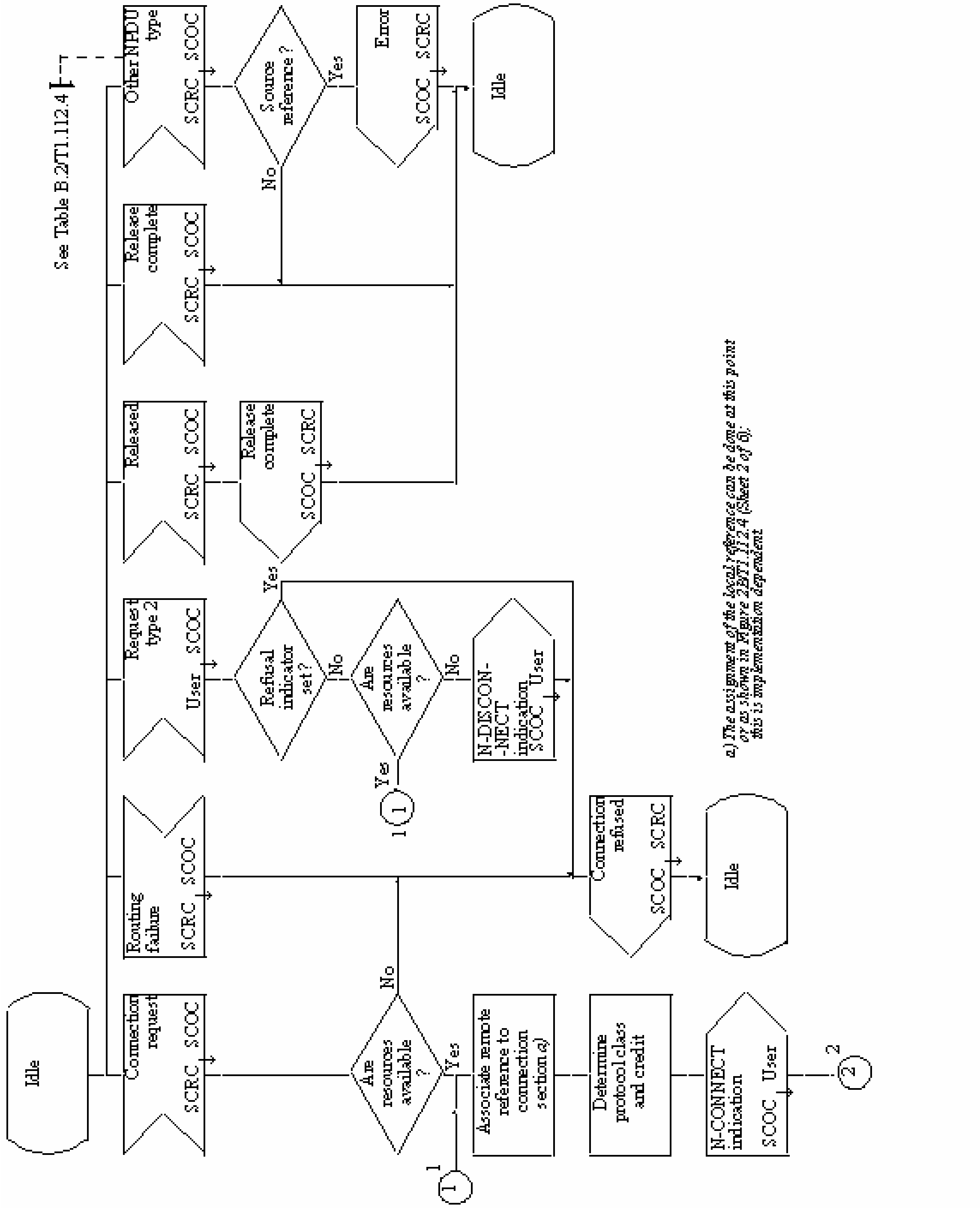


Figure 2B/ATIS-1000112.4 - SCOC, Connection establishment procedures at destination node (Sheet 1 of 6)

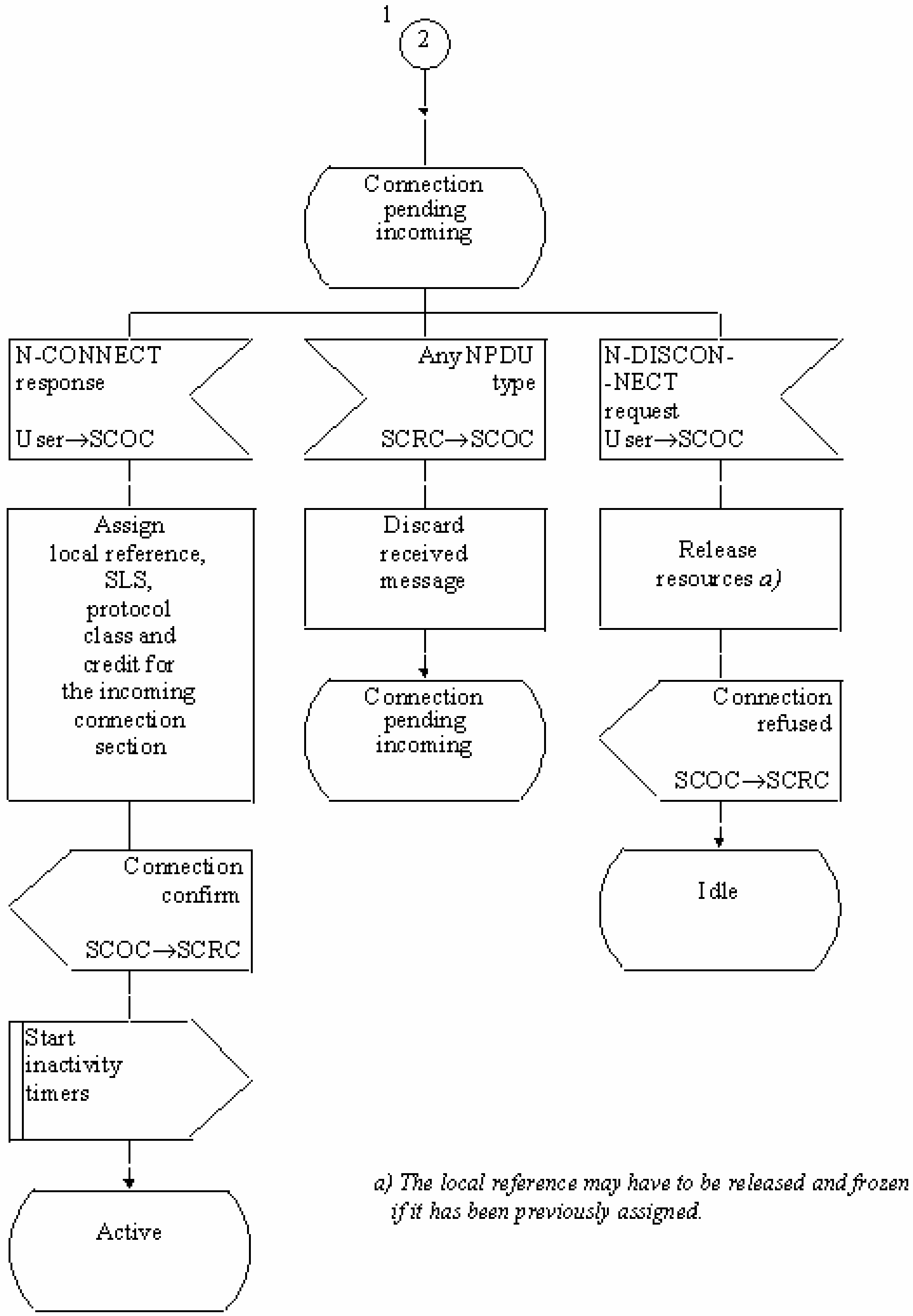


Figure 2B/ATIS-1000112.4 - SCOC, Connection establishment procedures at destination node (Sheet 2 of 6)

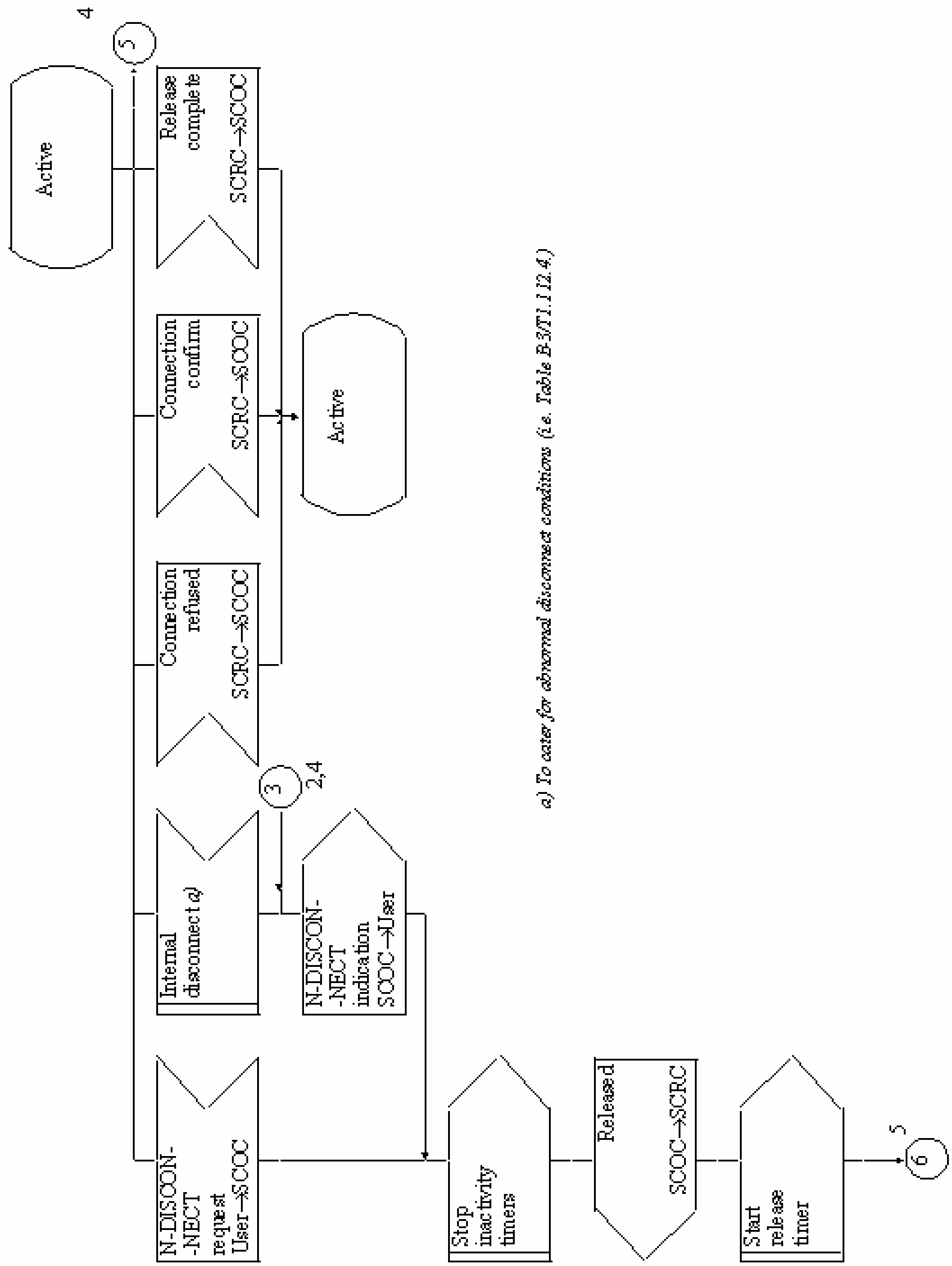


Figure 2B/ATIS-1000112.4 - SCOC, Connection release procedures at destination node (Sheet 3 of 6)

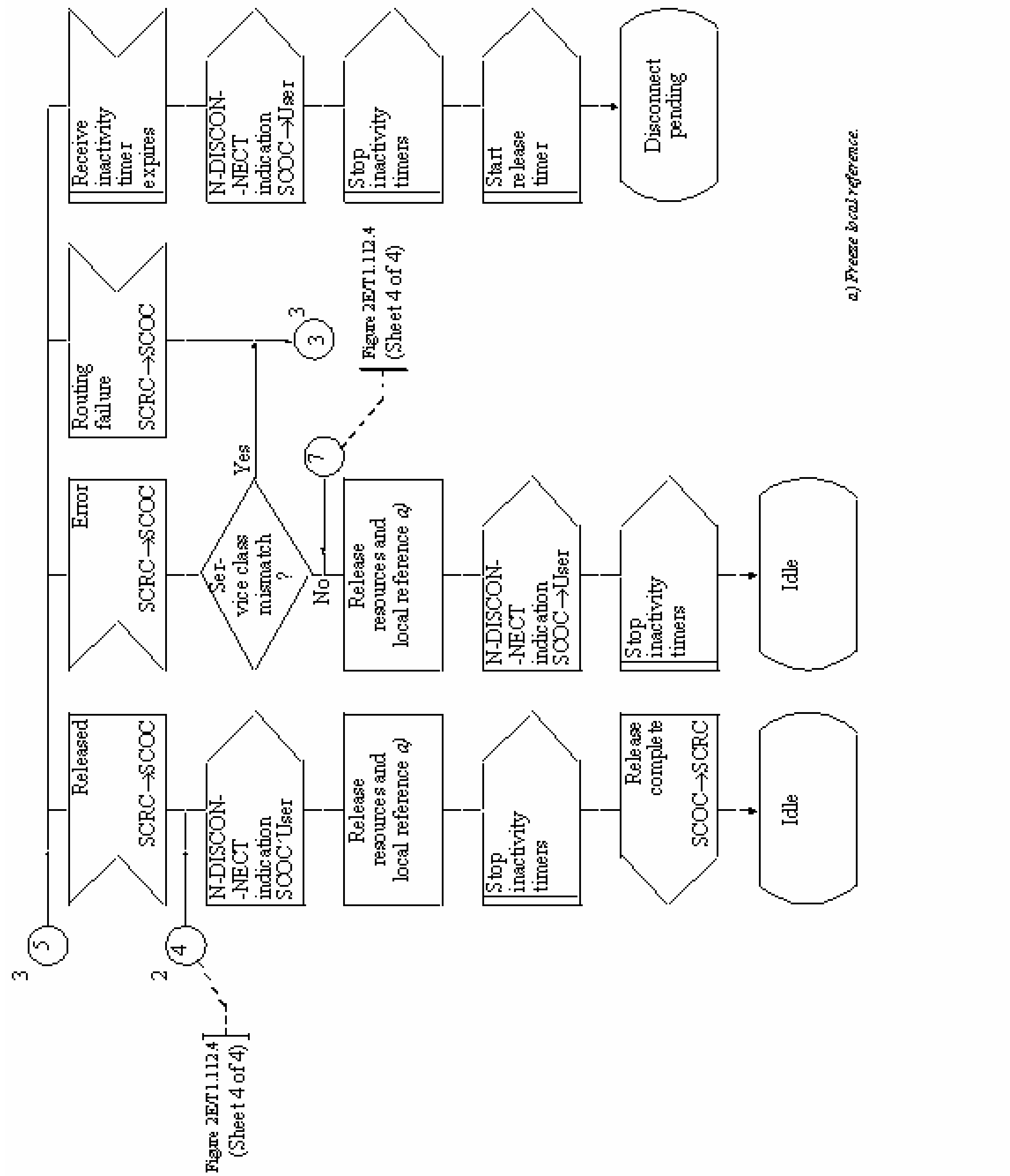


Figure 2B/ATIS-1000112.4 - SCOC, Connection release procedures at destination node (Sheet 4 of 6)

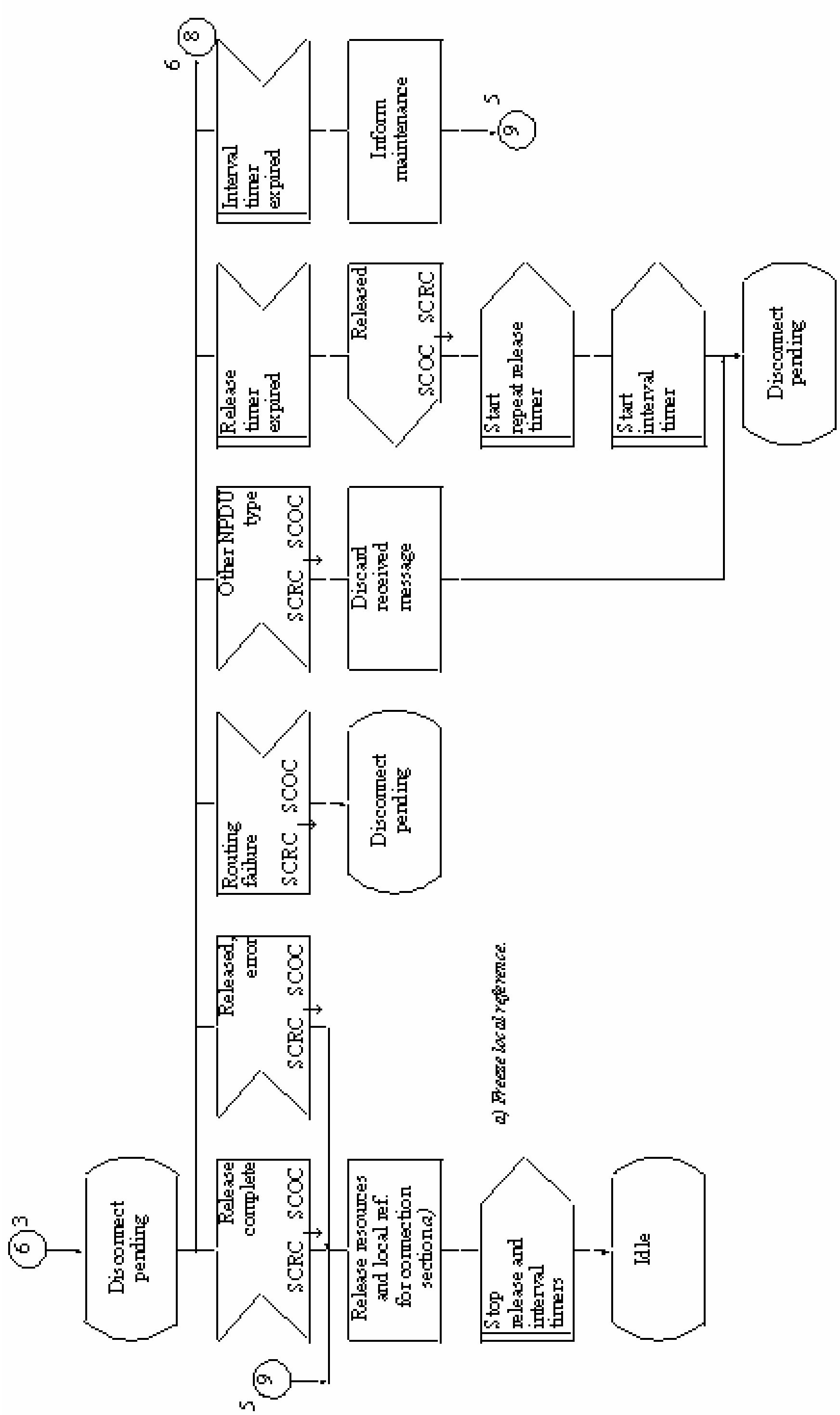


Figure 2B/ATIS-1000112.4 - SCOC, Connection release procedures at destination node (Sheet 5 of 6)

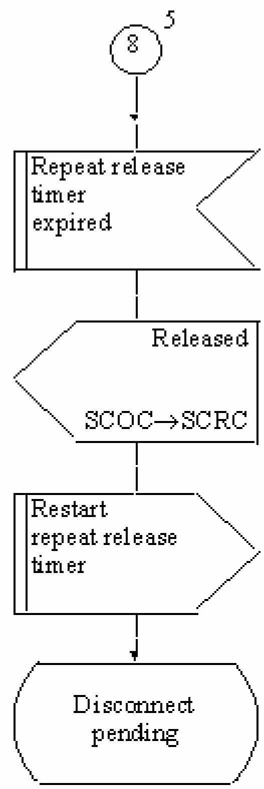


Figure 2B/ATIS-1000112.4 - SCOC, Connection release procedures at destination node (Sheet 6 of 6)

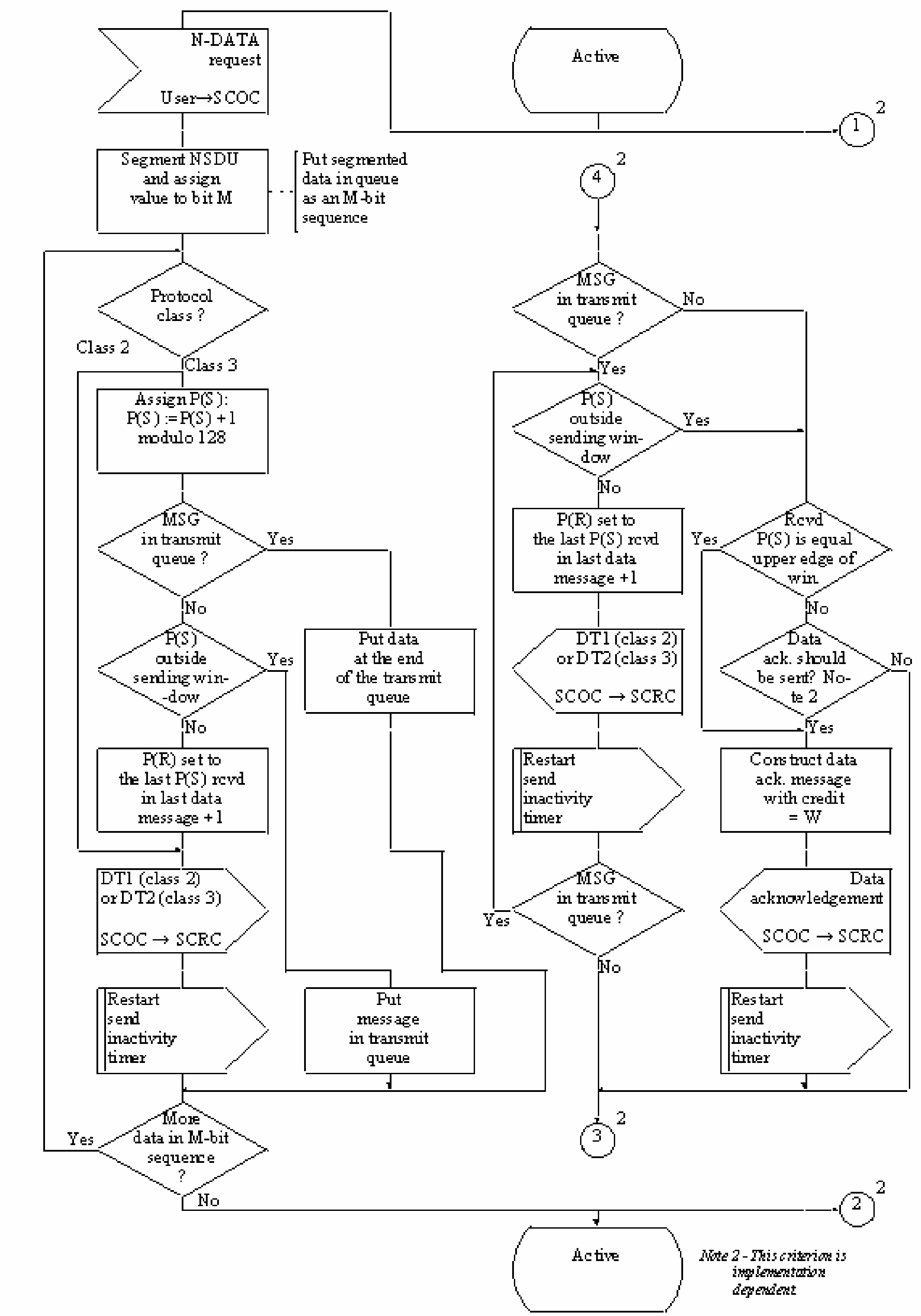


Figure 2C/ATIS-1000112.4 - SCOC, Data transfer procedures at originating and destination nodes
(Sheet 1 of 4)

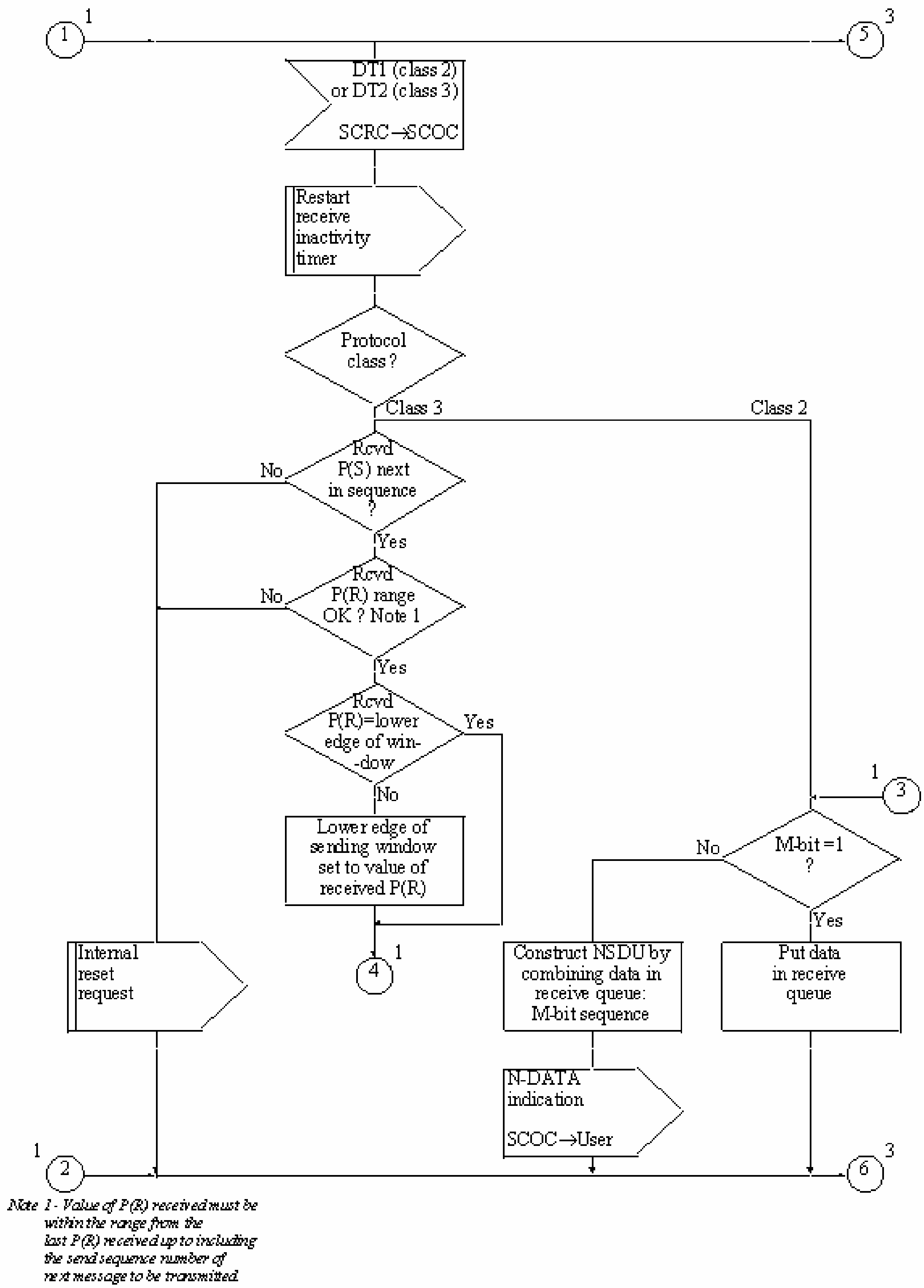


Figure 2C/ATIS-1000112.4 - SCOC, Data transfer procedures at originating and destination nodes
(Sheet 2 of 4)

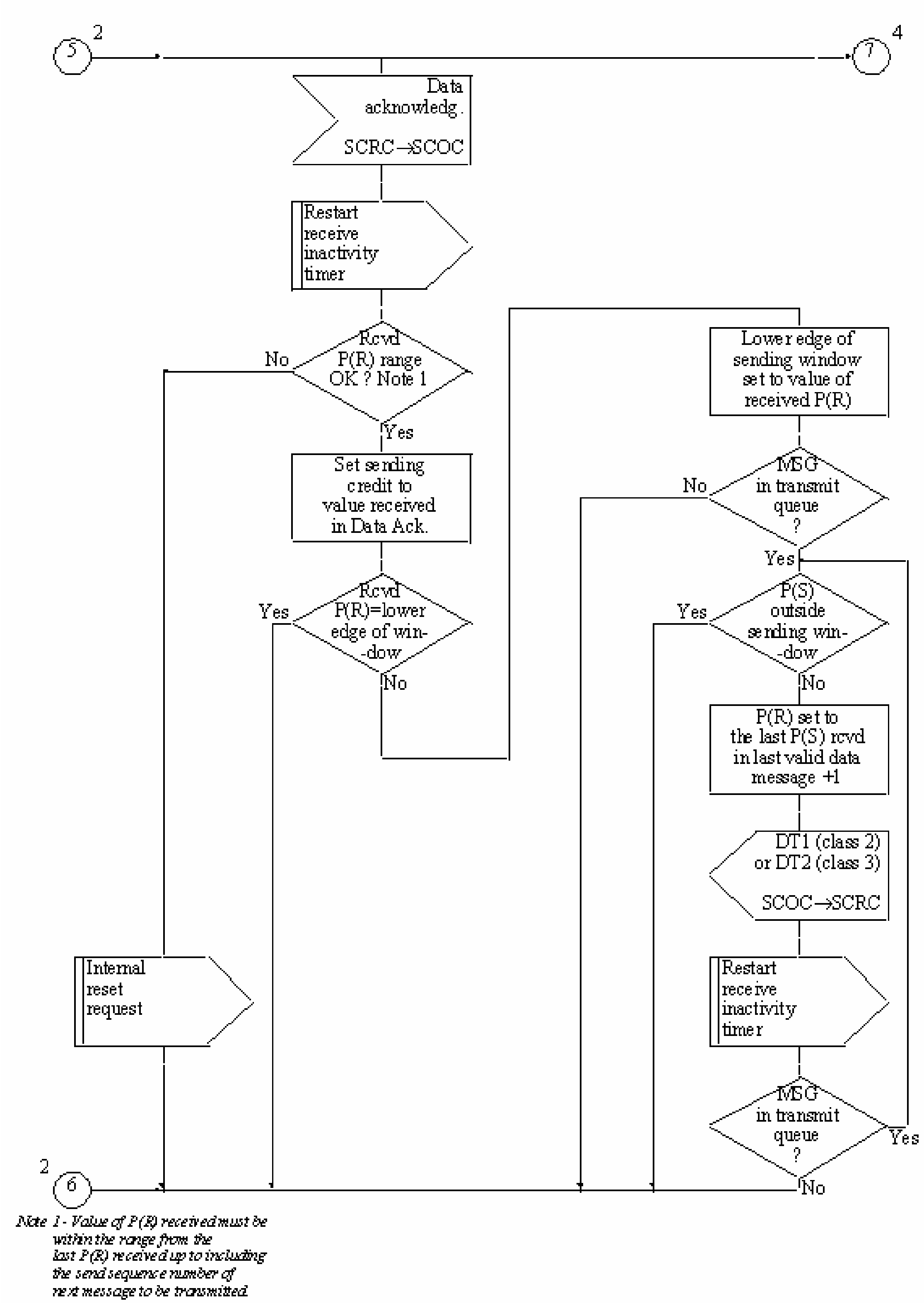


Figure 2C/ATIS-1000112.4 - SCOC, Data transfer procedures at originating and destination nodes (Sheet 3 of 4)

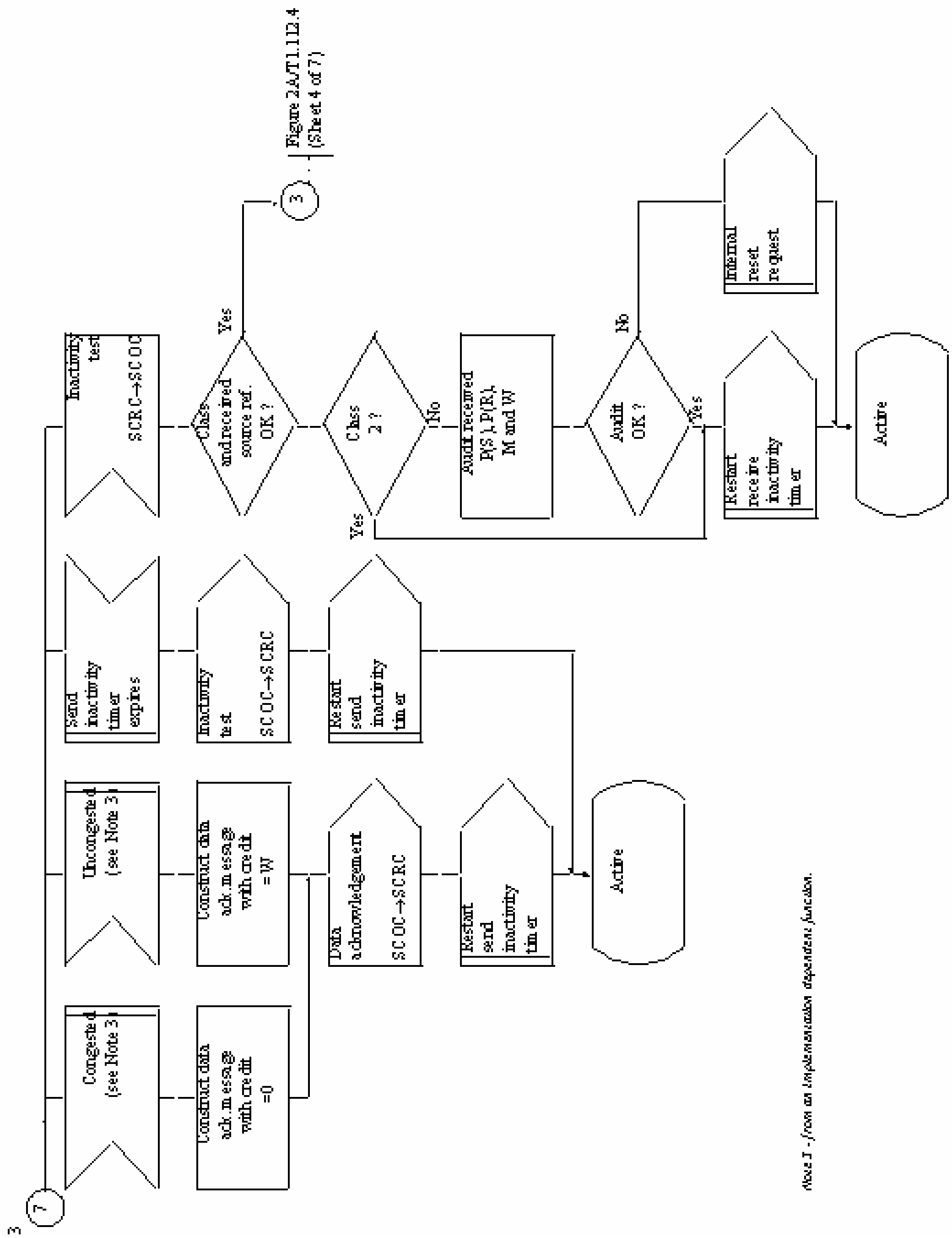


Figure 2C/ATIS-1000112.4 - SCOC, Data transfer procedures at originating and destination nodes
(Sheet 4 of 4)

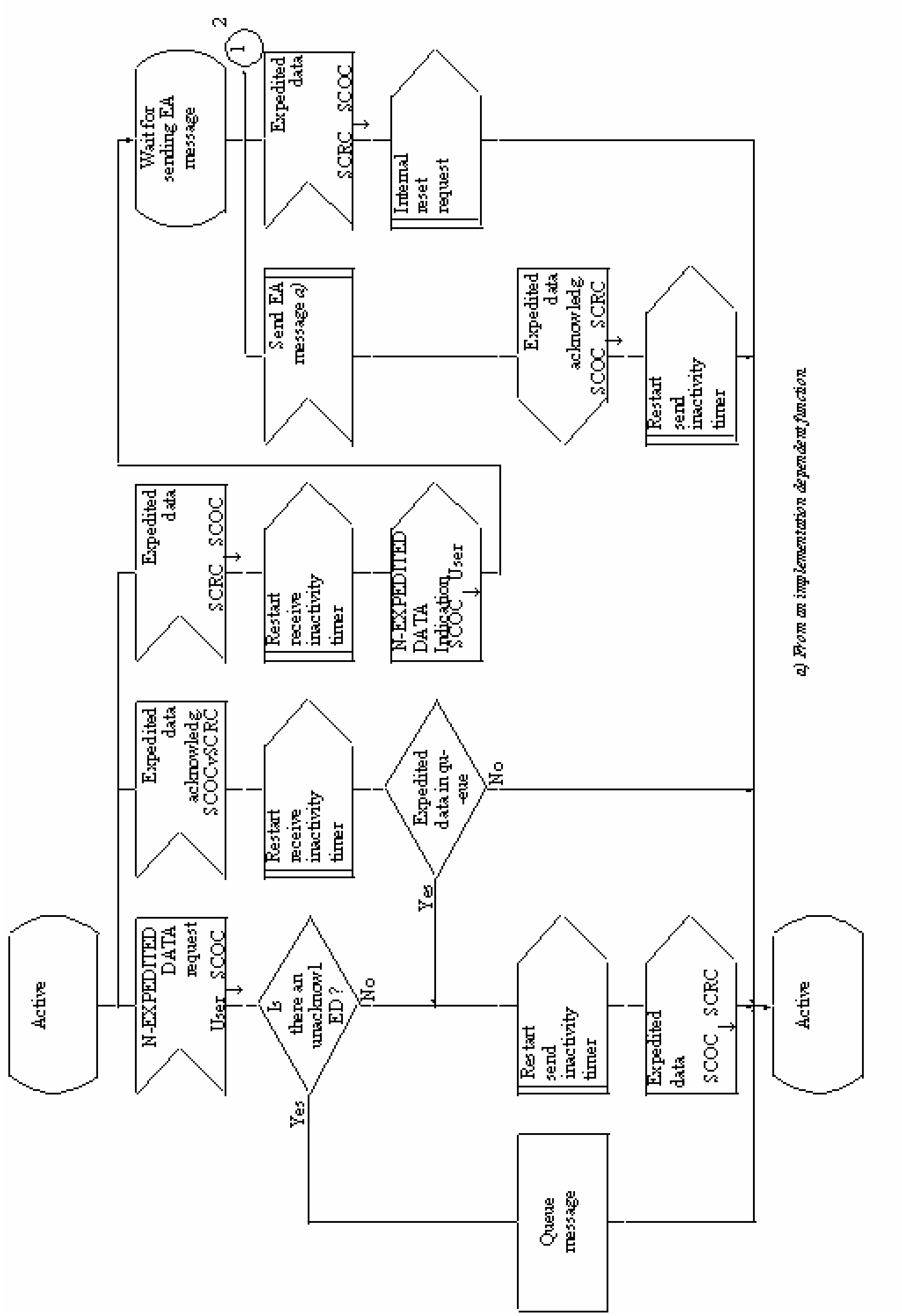


Figure 2D/ATIS-1000112.4 - SCOC, Expedited data transfer procedures at originating and destination node (Sheet 1 of 2)

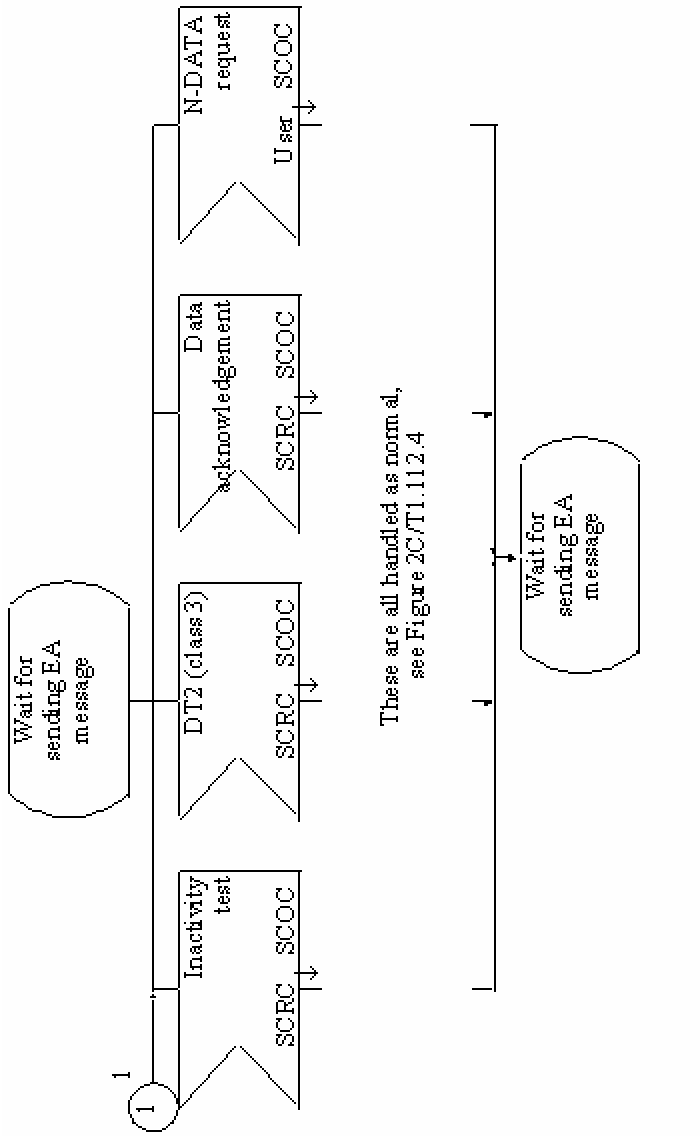


Figure 2D/ATIS-1000112.4 - SCOC, Expedited data transfer procedures at originating and destination node (Sheet 2 of 2)

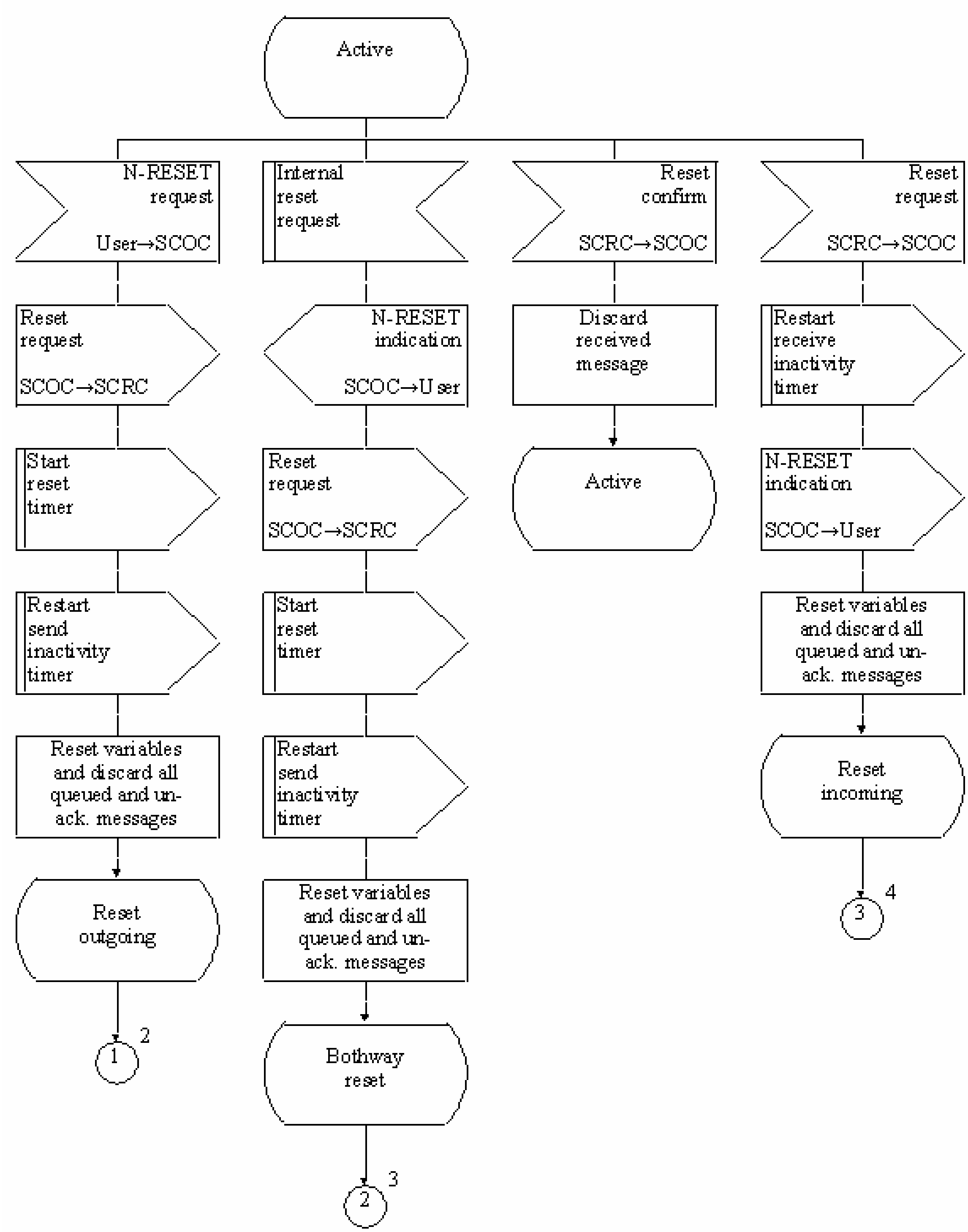


Figure 2E/ATIS-1000112.4 - SCOC, Reset procedures at originating and destination node (Sheet 1 of 4)

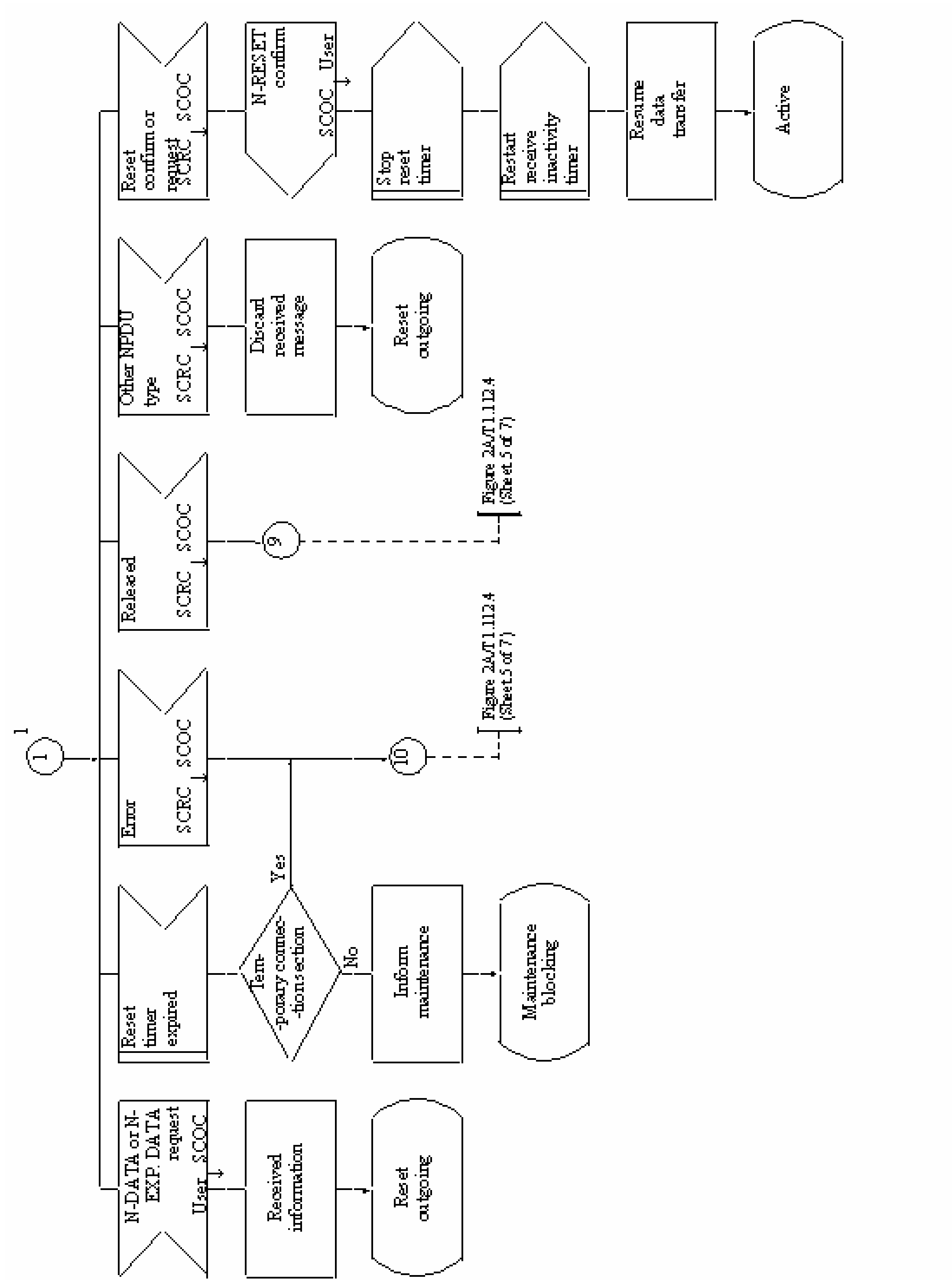


Figure 2E/ATIS-1000112.4 - SCOC, Reset procedures at originating and destination node (Sheet 2 of 4)

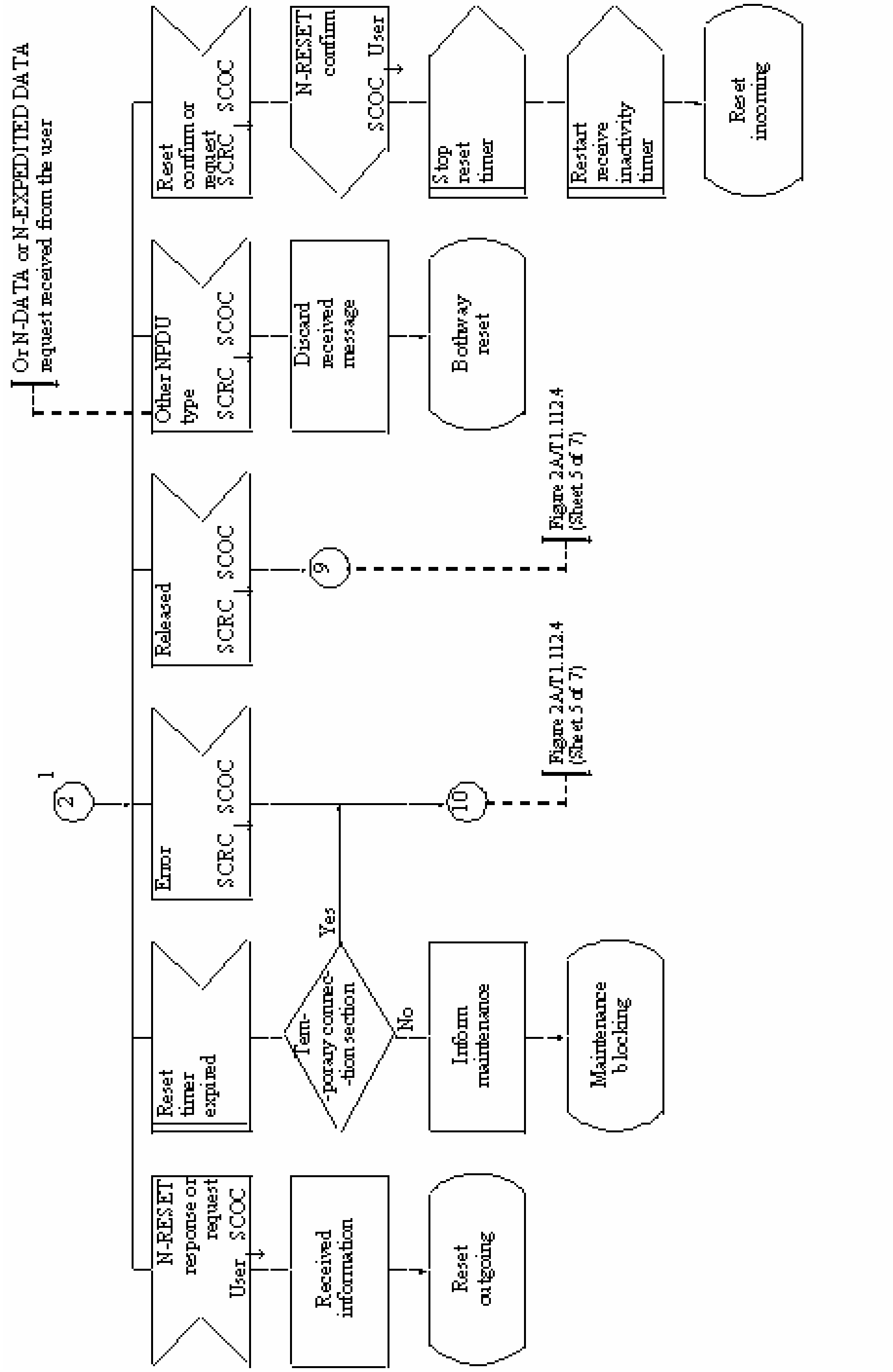


Figure 2E/ATIS-1000112.4 - SCOC, Reset procedures at originating and destination node (Sheet 3 of 4)

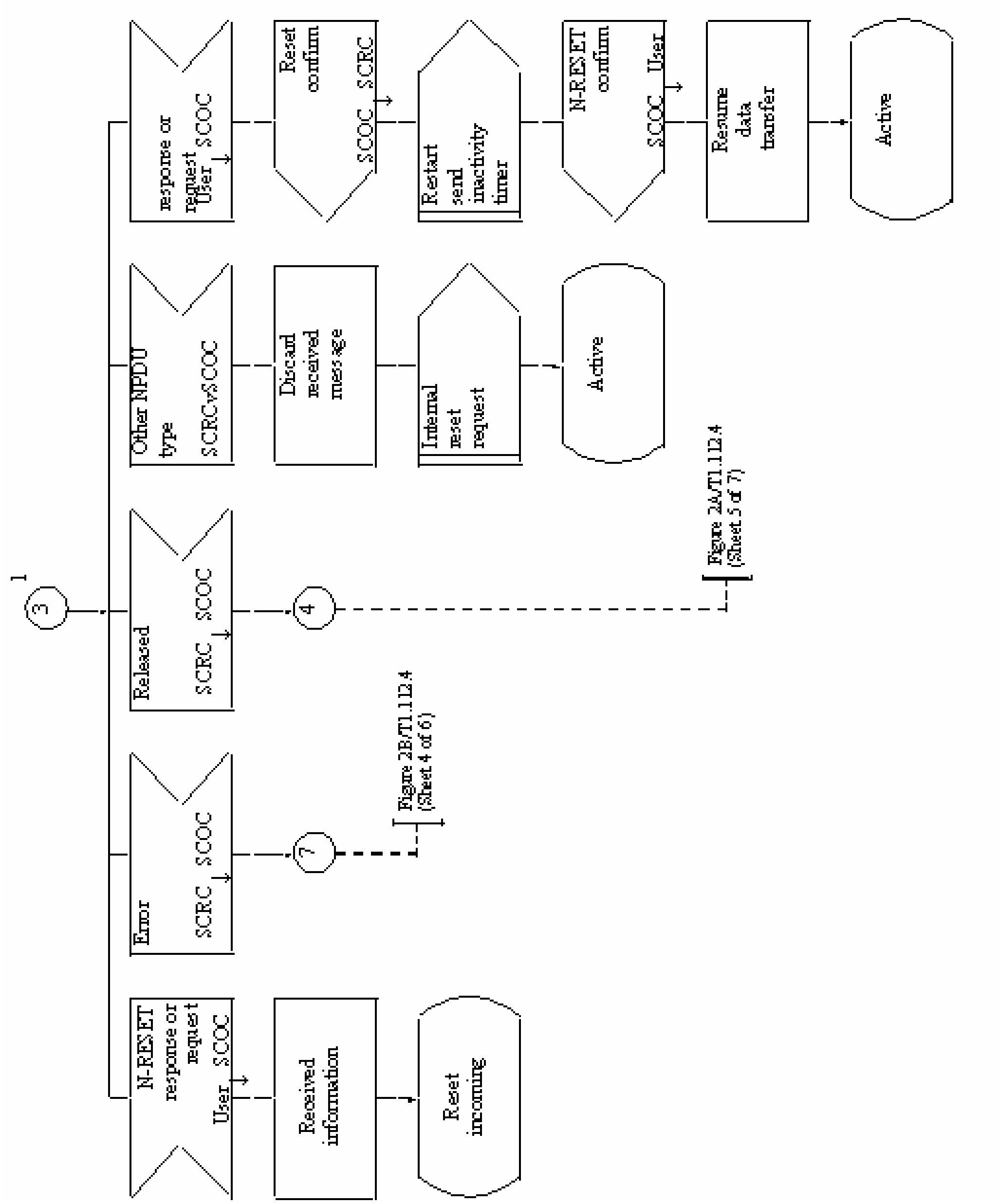


Figure 2E/ATIS-1000112.4 - SCOC, Reset procedures at originating and destination node (Sheet 4 of 4)

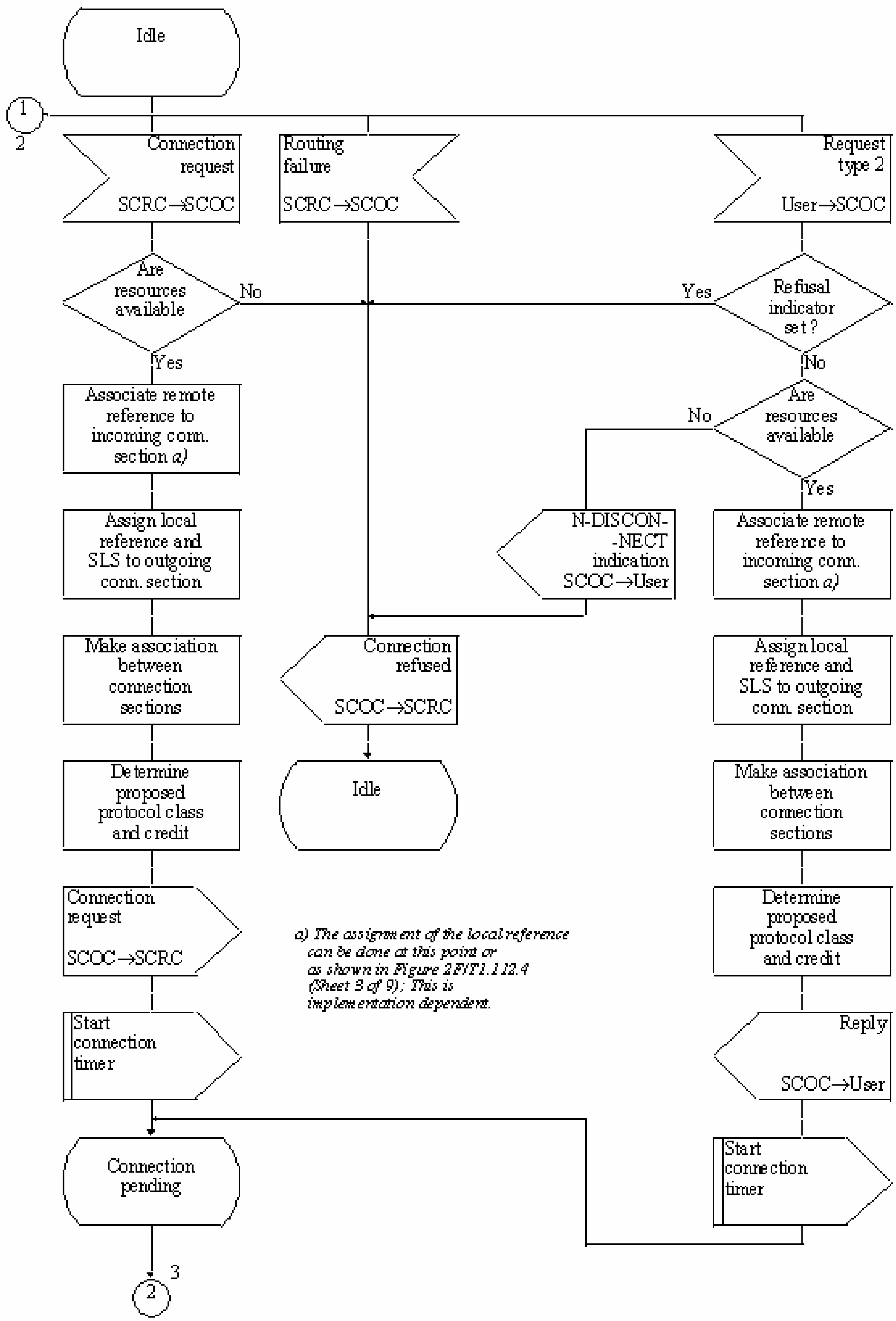


Figure 2F/ATIS-1000112.4 - SCOC, Connection establishment procedures at relay node with coupling (Sheet 1 of 9)

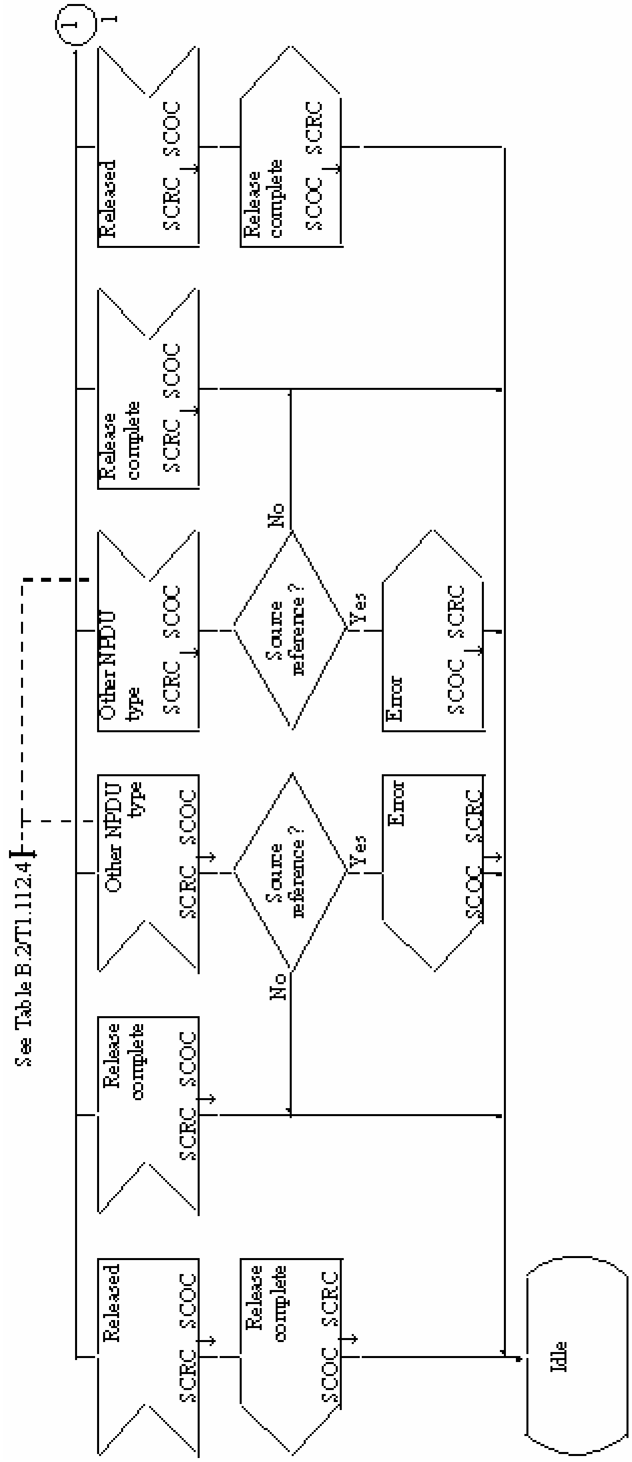


Figure 2F/ATIS-1000112.4 - SCOC, Connection establishment procedures at relay node with coupling (Sheet 2 of 9)

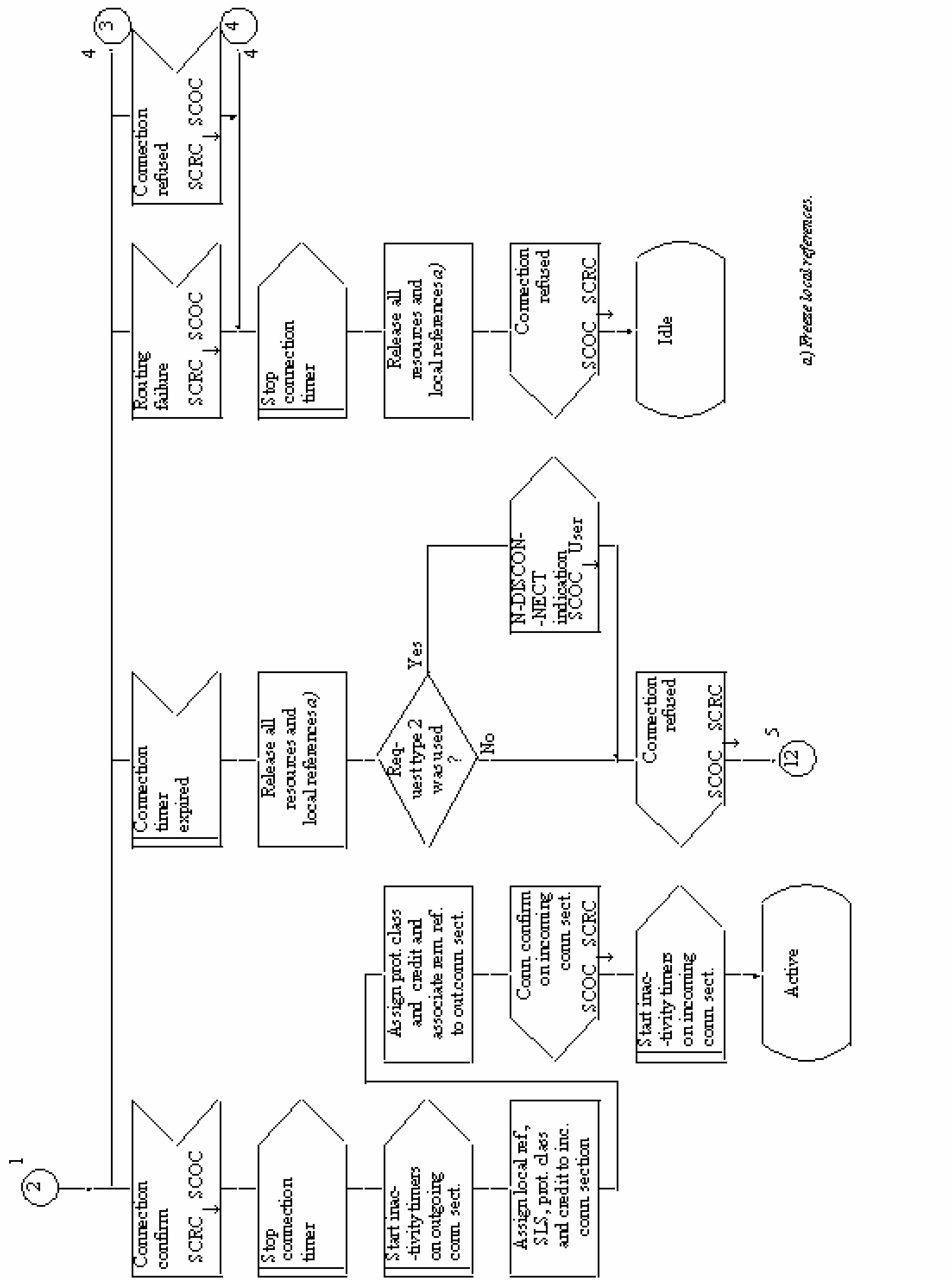


Figure 2F/ATIS-1000112.4 - SCOC, Connection establishment procedures at relay node with coupling (Sheet 3 of 9)

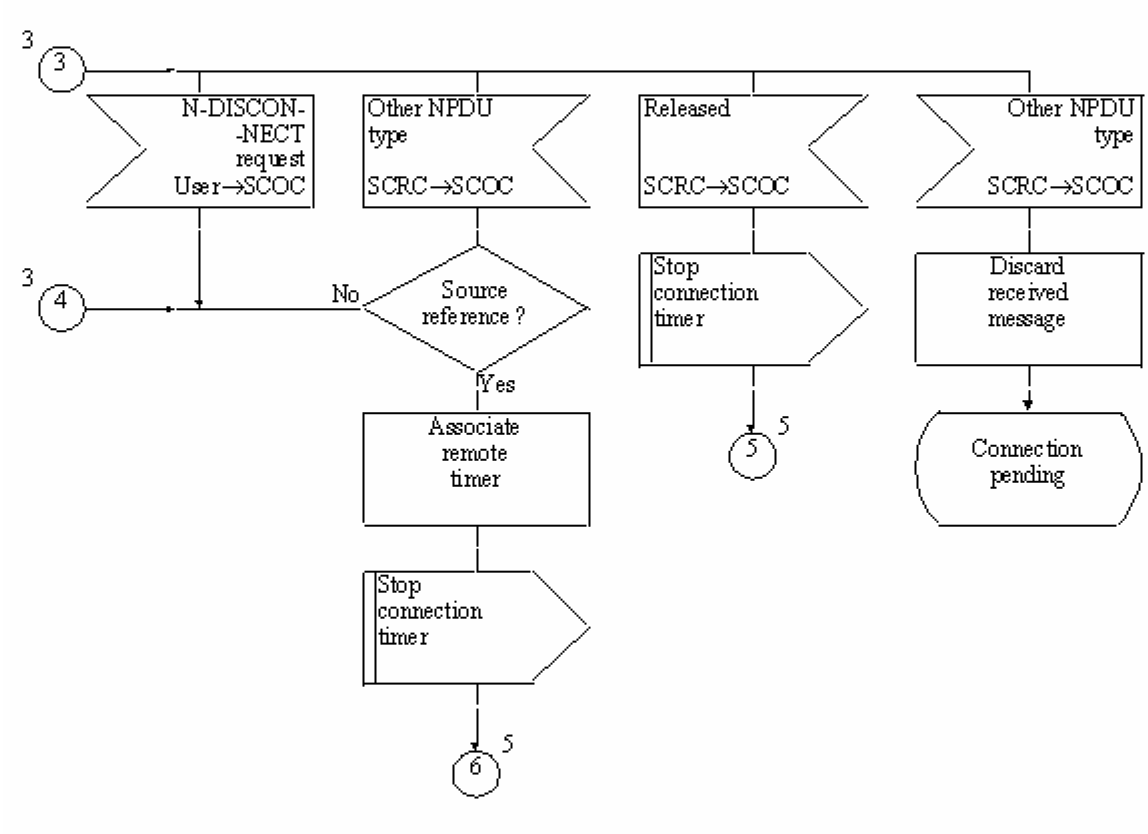
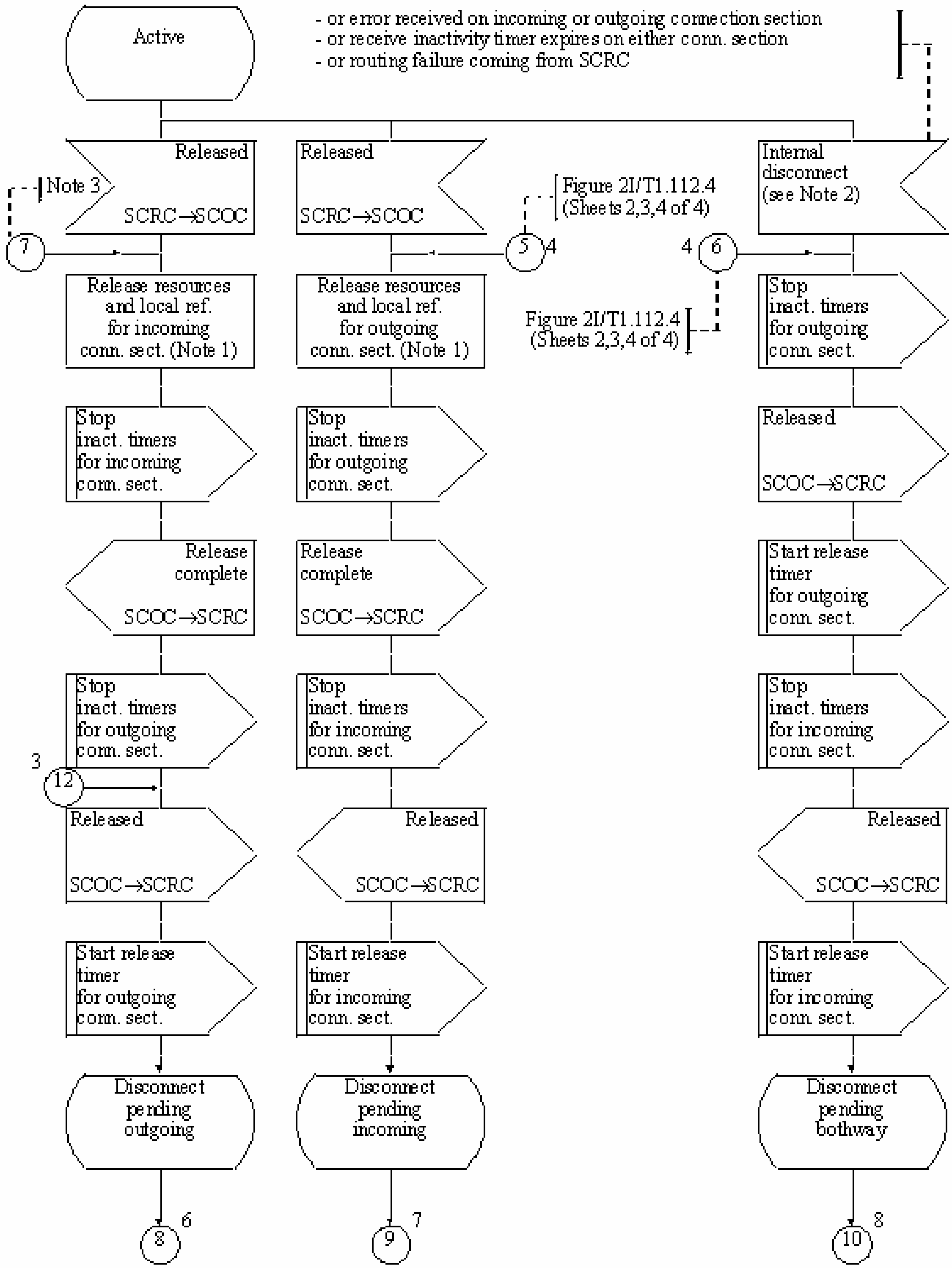


Figure 2F/ATIS-1000112.4 - SCOC, Connection establishment procedures at relay node with coupling (Sheet 4 of 9)



Note 1 - Freeze local references.
Note 2 - To cater for abnormal disconnect conditions (i.e. Table B-3/T1.112.4).
Note 3 - Figure 2I/T1.112.4 (Sheets 2,3,4 of 4).

Figure 2F/ATIS-1000112.4 - SCOC, Connection release procedures at relay node with coupling (Sheet 5 of 9)

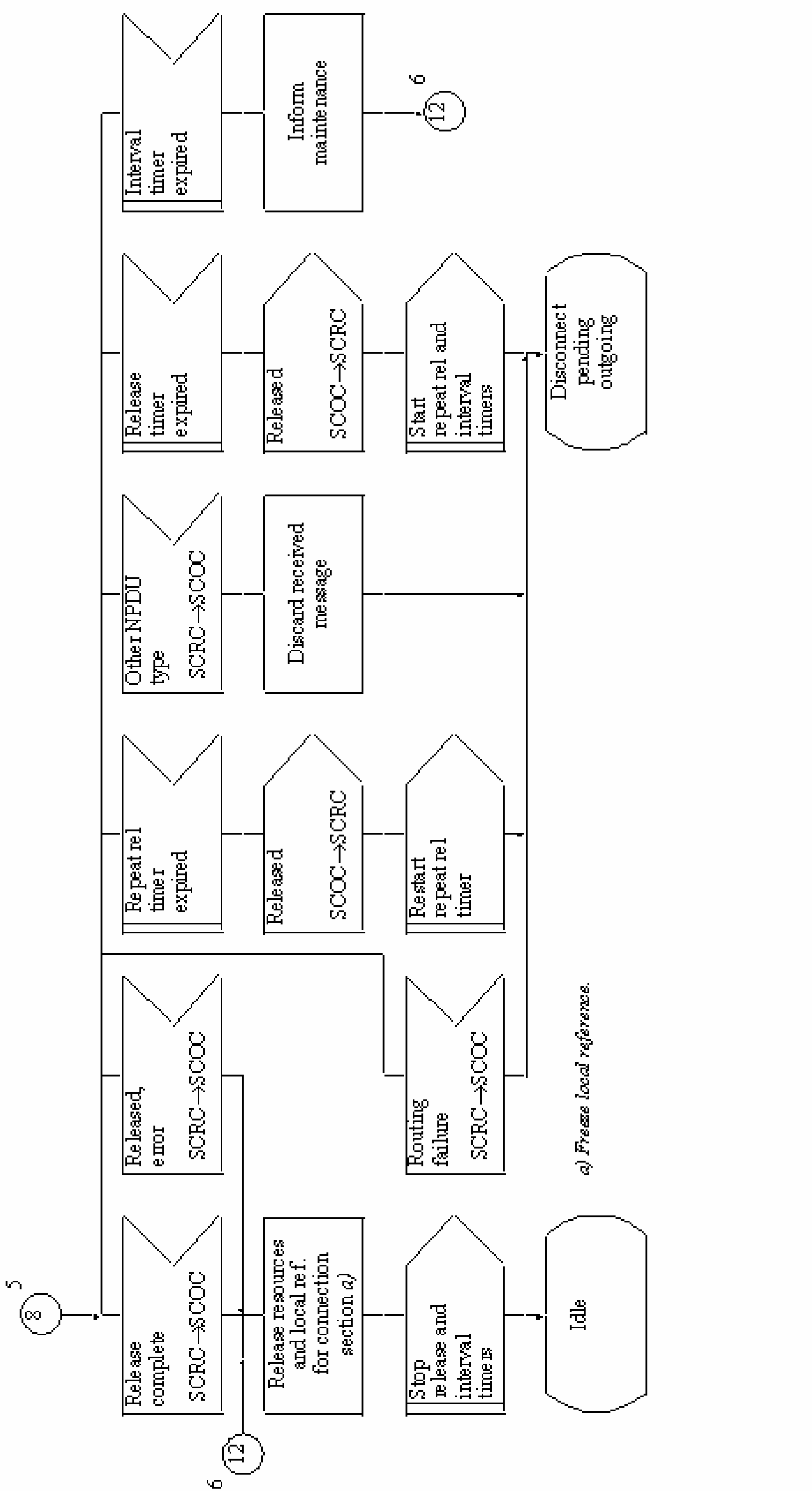


Figure 2F/ATIS-1000112.4 - SCOC, Connection release procedures at relay node with coupling (Sheet 6 of 9)

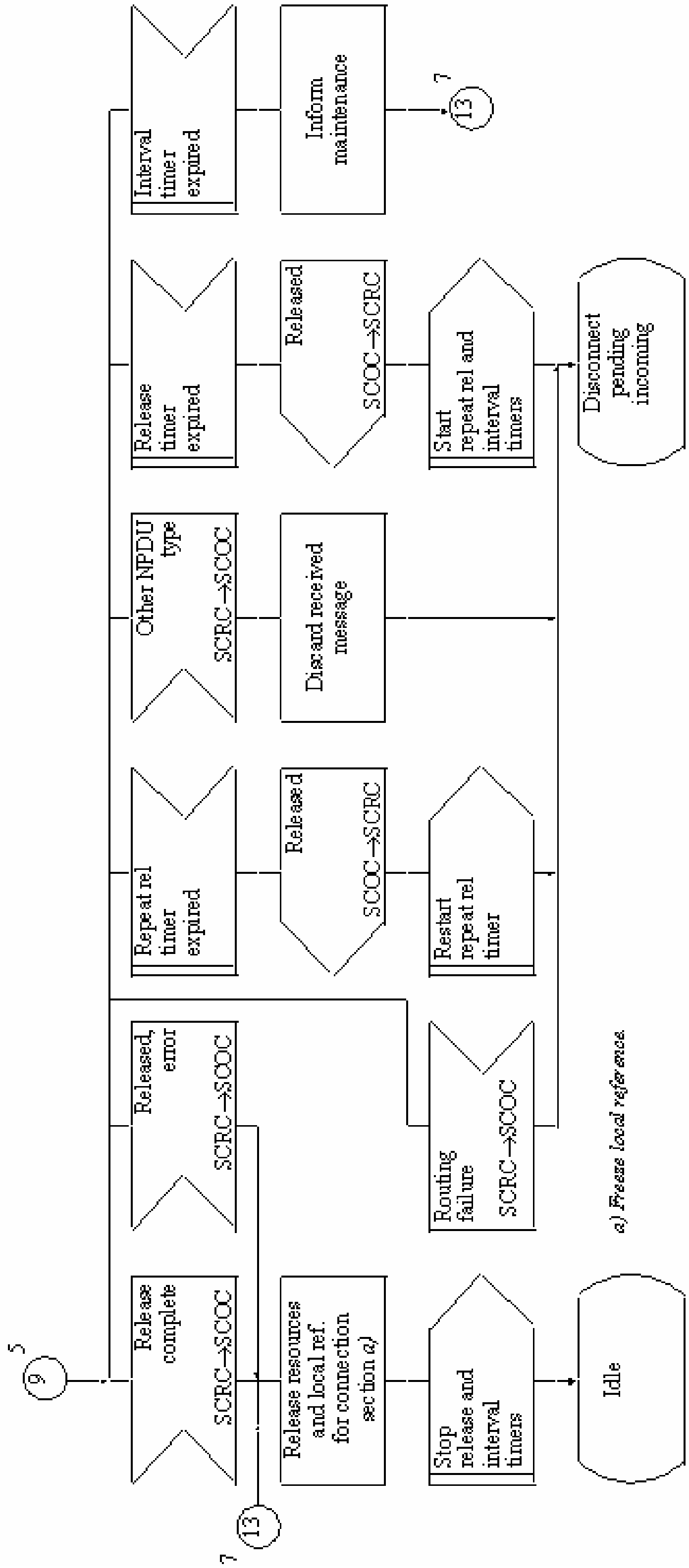


Figure 2F/ATIS-1000112.4 - SCOC, Connection release procedures at relay node with coupling (Sheet 7 of 9)

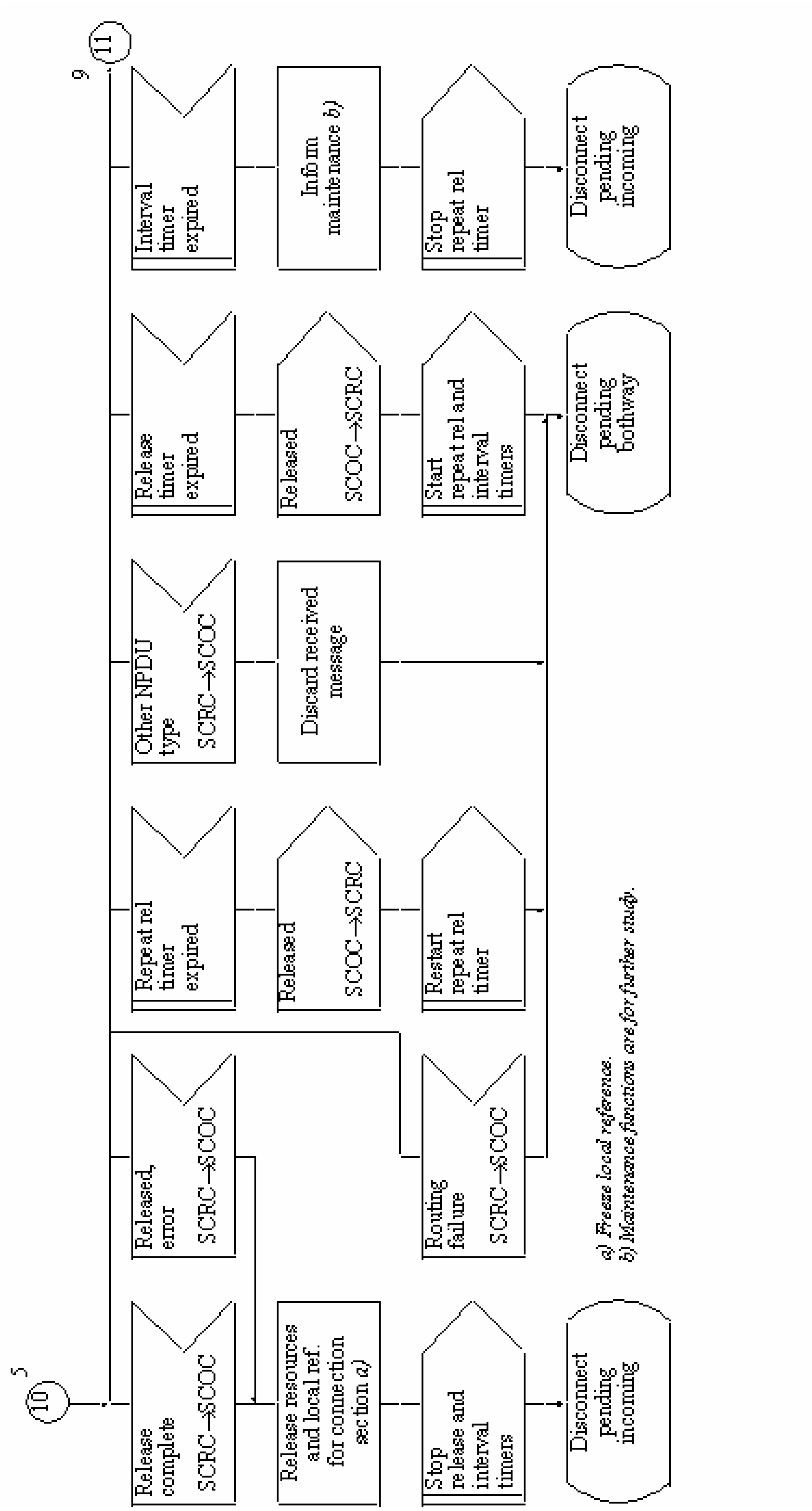


Figure 2F/ATIS-1000112.4 - SCOC, Connection release procedures at relay node with coupling (Sheet 8 of 9)

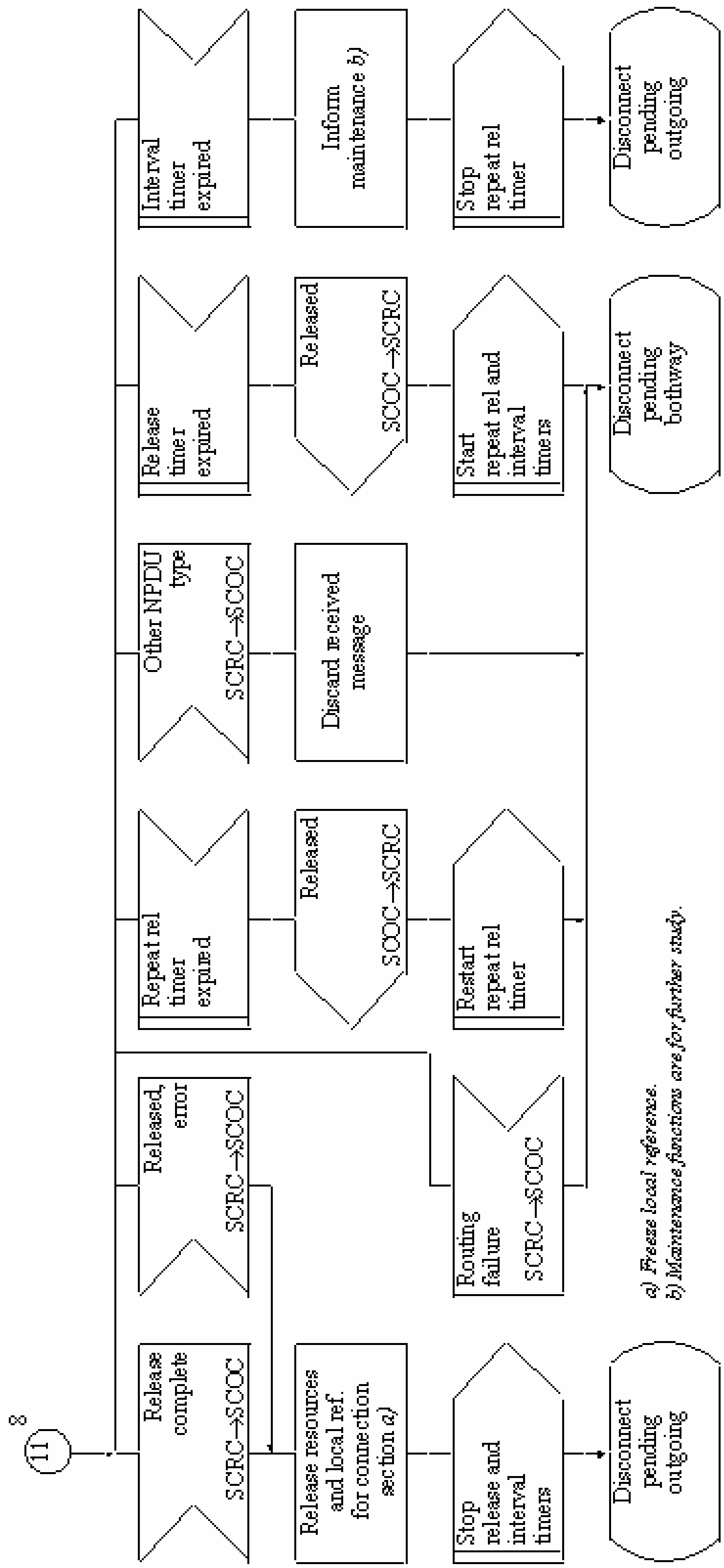


Figure 2F/ATIS-1000112.4 - SCOC, Connection release procedures at relay node with coupling (Sheet 9 of 9)

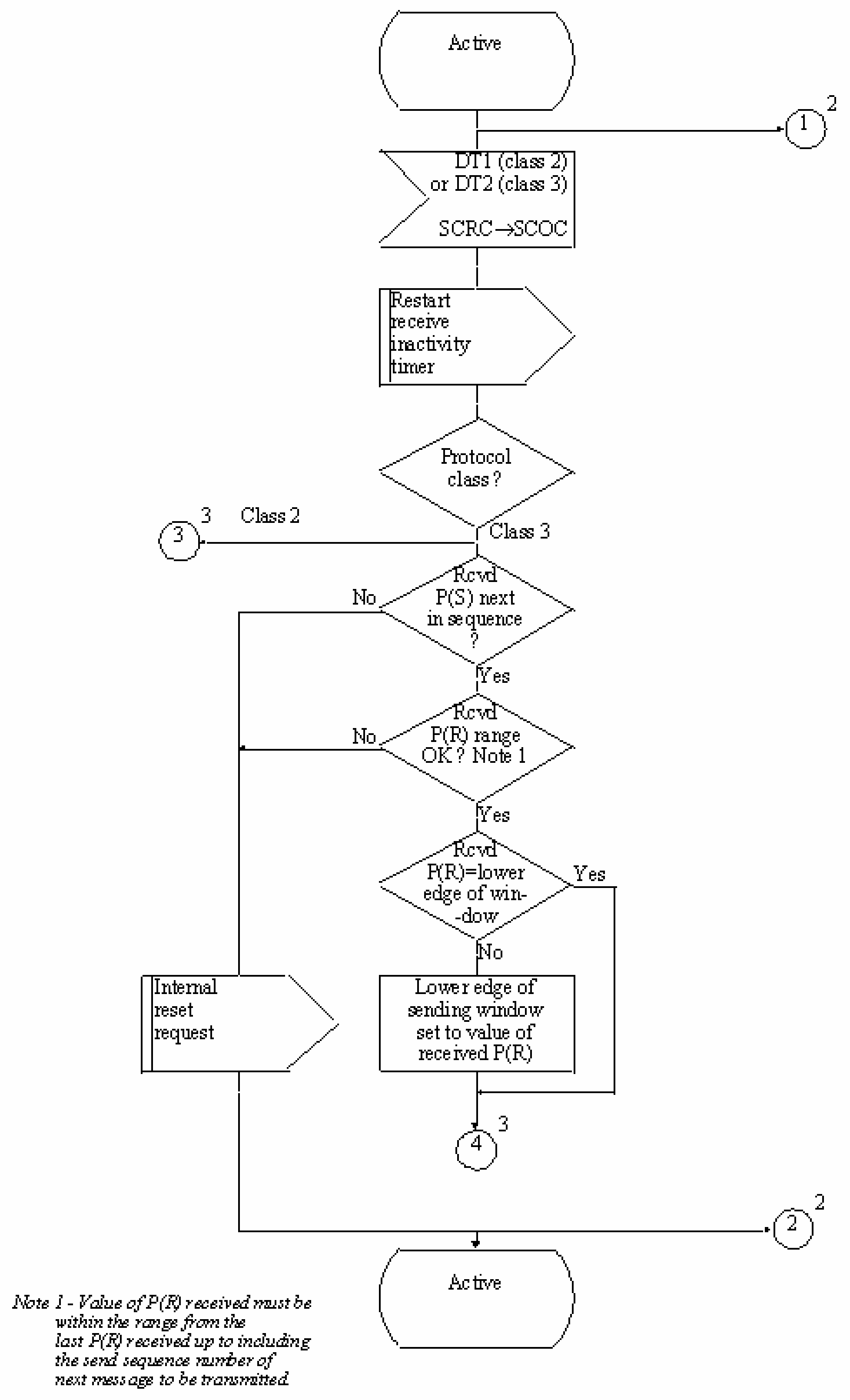


Figure 2G/ATIS-1000112.4 - SCOC, Data transfer procedures at relay node with coupling (Sheet 1 of 4)

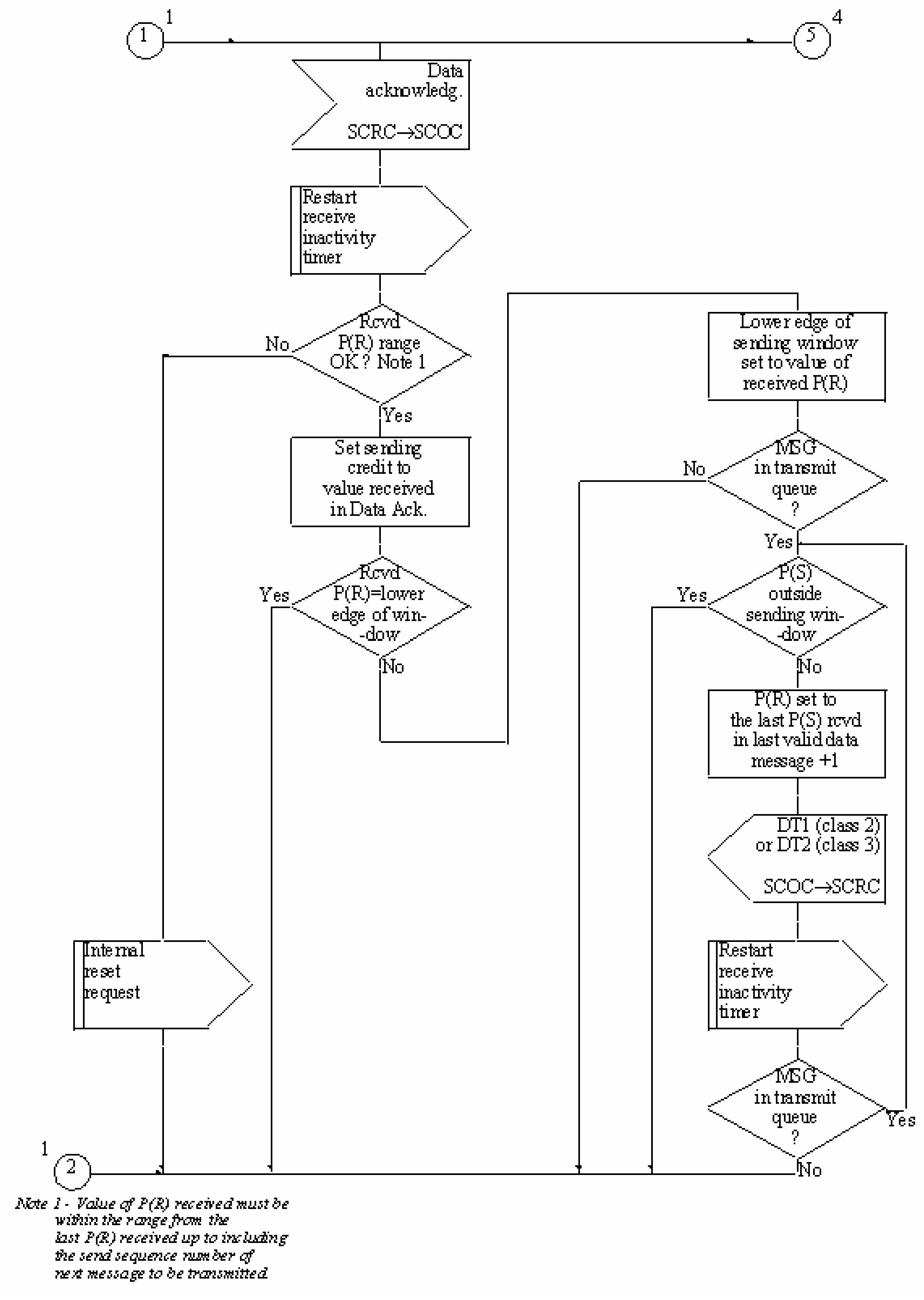


Figure 2G/ATIS-1000112.4 - SCOC, Data transfer procedures at relay node with coupling (Sheet 2 of 4)

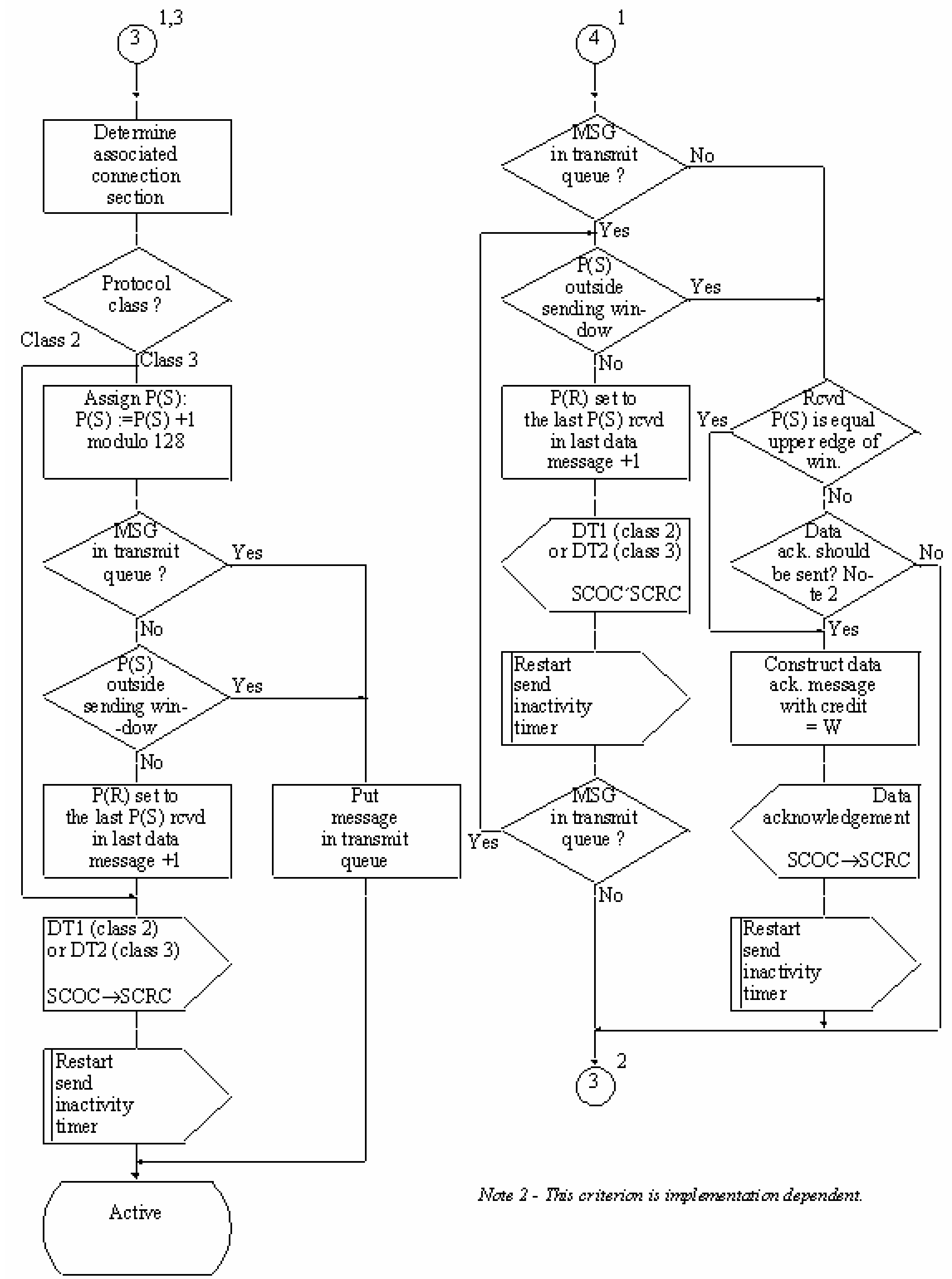


Figure 2G/ATIS-1000112.4 - SCOC, Data transfer procedures at relay node with coupling (Sheet 3 of 4)

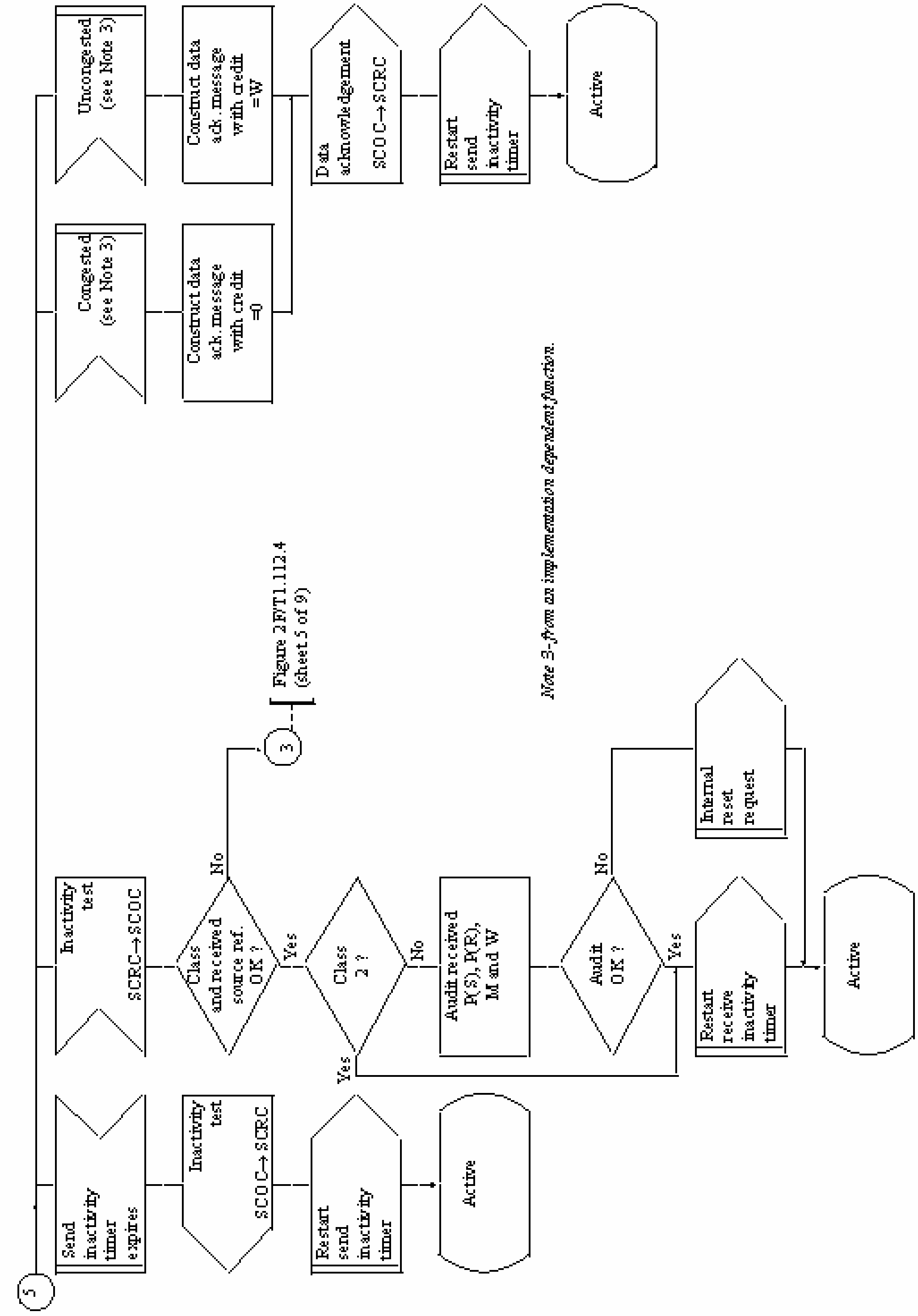


Figure 2G/ATIS-1000112.4 - SCOC, Data transfer procedures at relay node with coupling (Sheet 4 of 4)

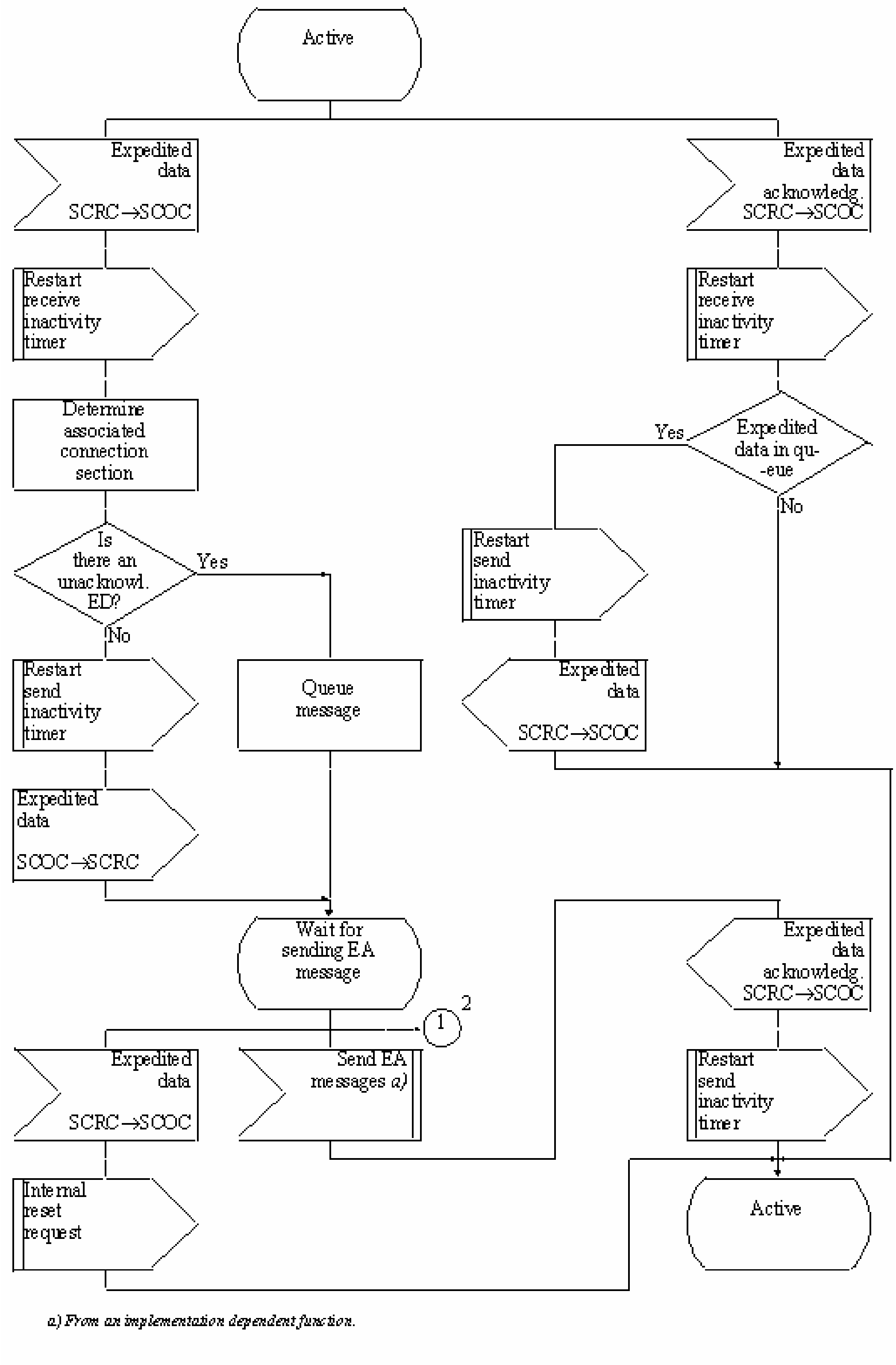


Figure 2H/ATIS-1000112.4 - SCOC, Expedited data transfer at relay node with coupling (Sheet 1 of 2)

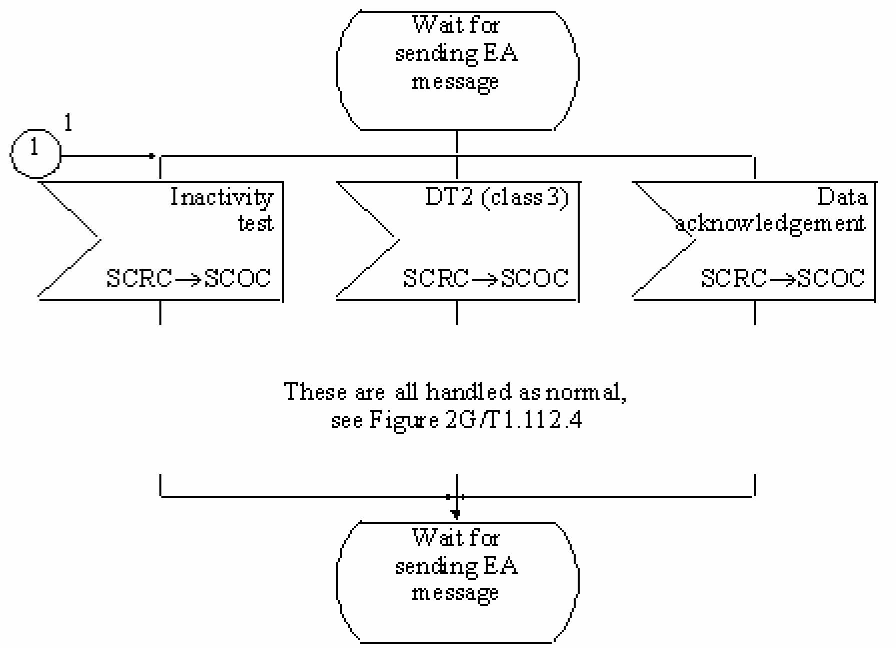


Figure 2H/ATIS-1000112.4 - SCOC, Expedited data transfer at relay node with coupling (Sheet 2 of 2)

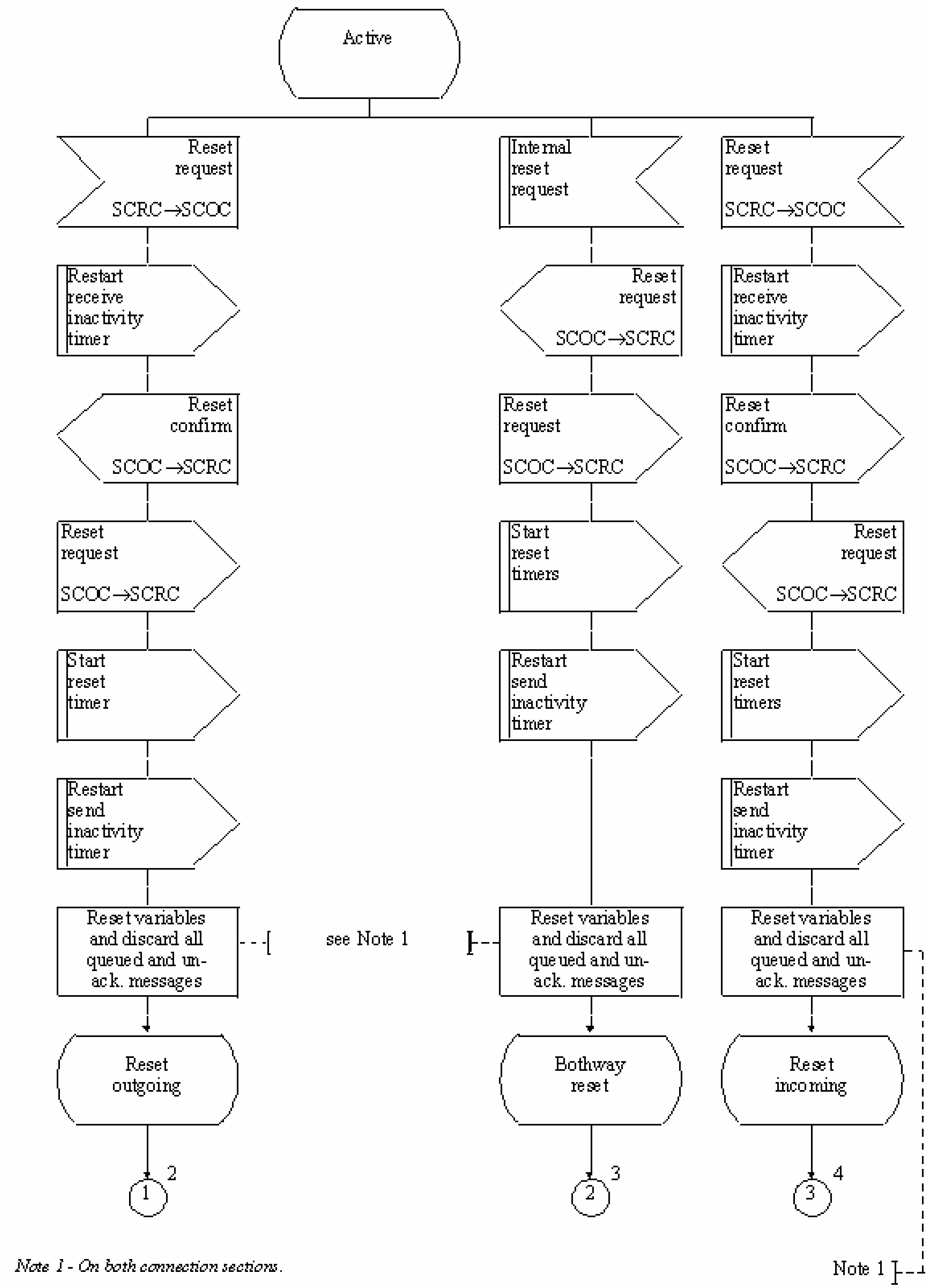


Figure 2I/ATIS-1000112.4 - SCOC, Reset procedures at relay node with coupling (Sheet 1 of 4)

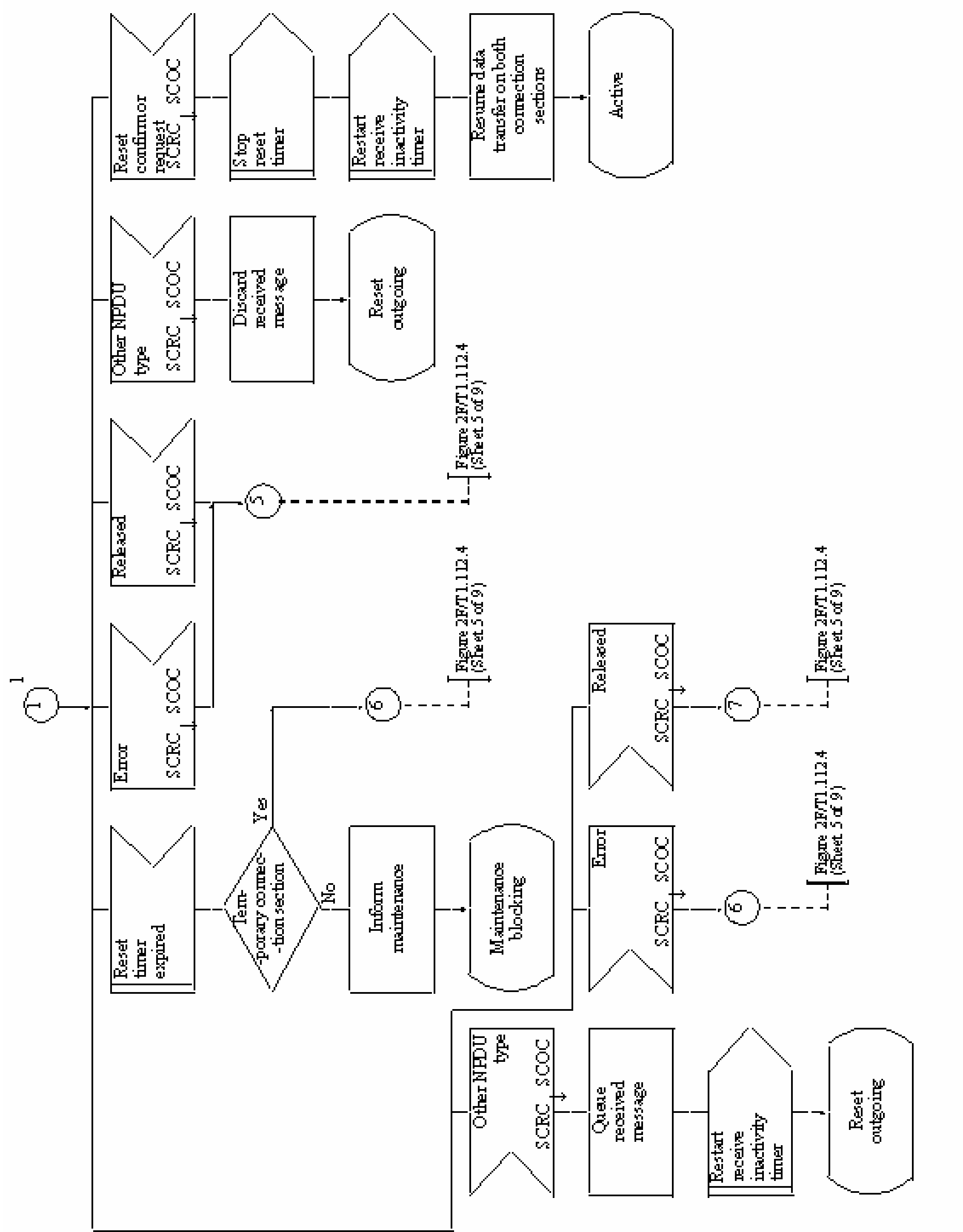


Figure 2I/ATIS-1000112.4 - SCOC, Reset procedures at relay node with coupling (Sheet 2 of 4)

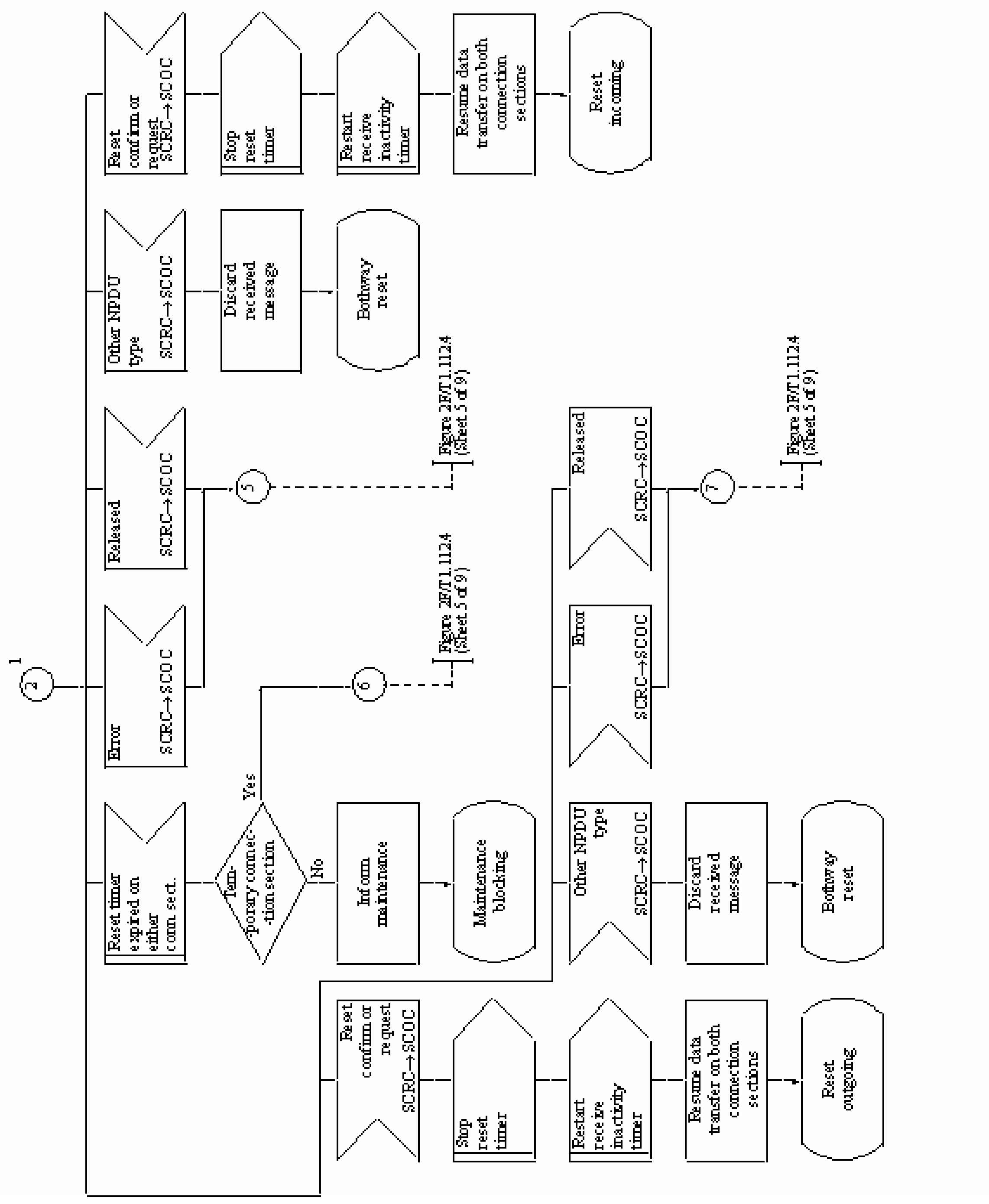


Figure 2I/ATIS-1000112.4 - SCOC, Reset procedures at relay node with coupling (Sheet 3 of 4)

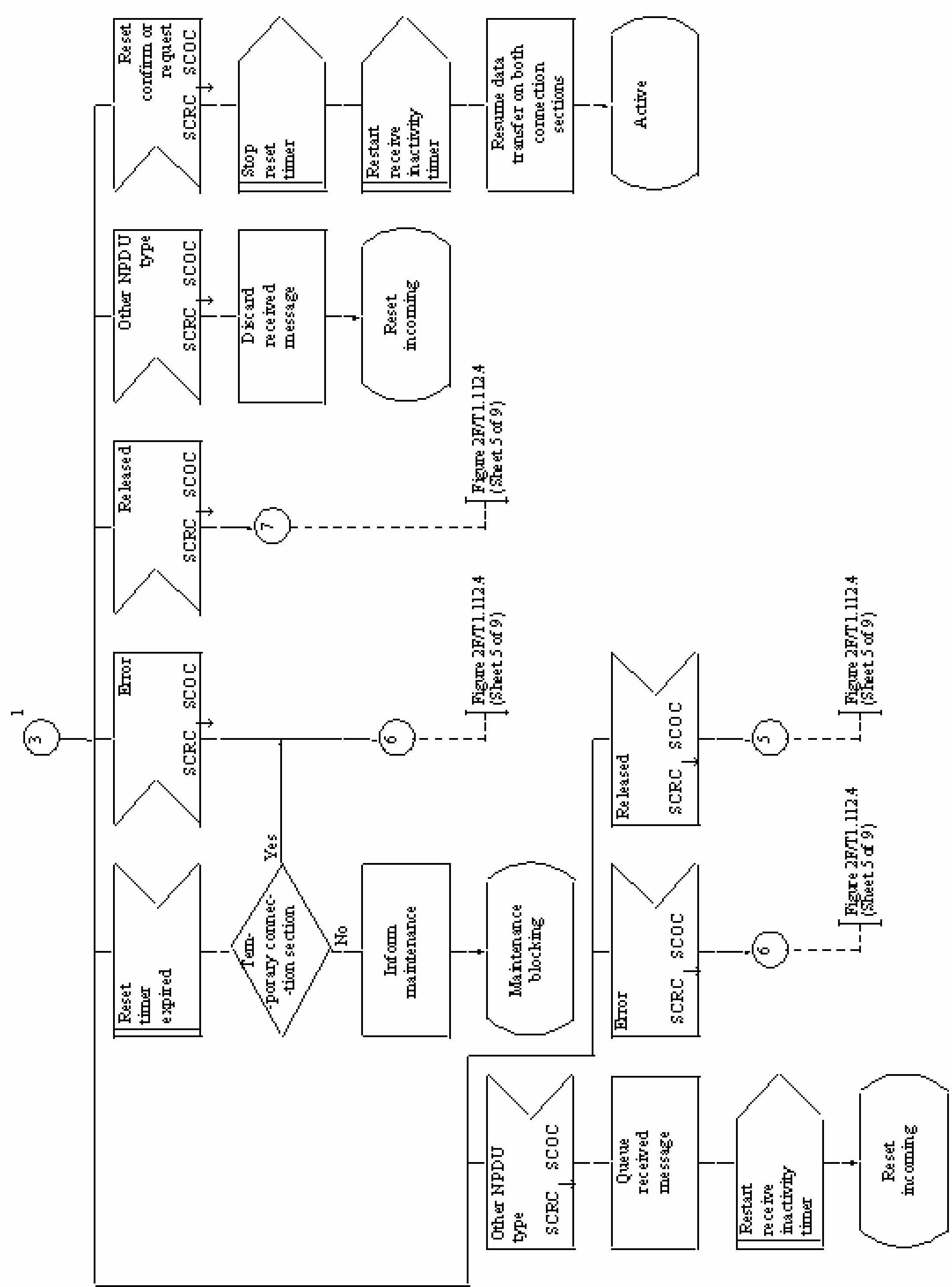


Figure 2I/ATIS-1000112.4 - SCOC, Reset procedures at relay node with coupling (Sheet 4 of 4)

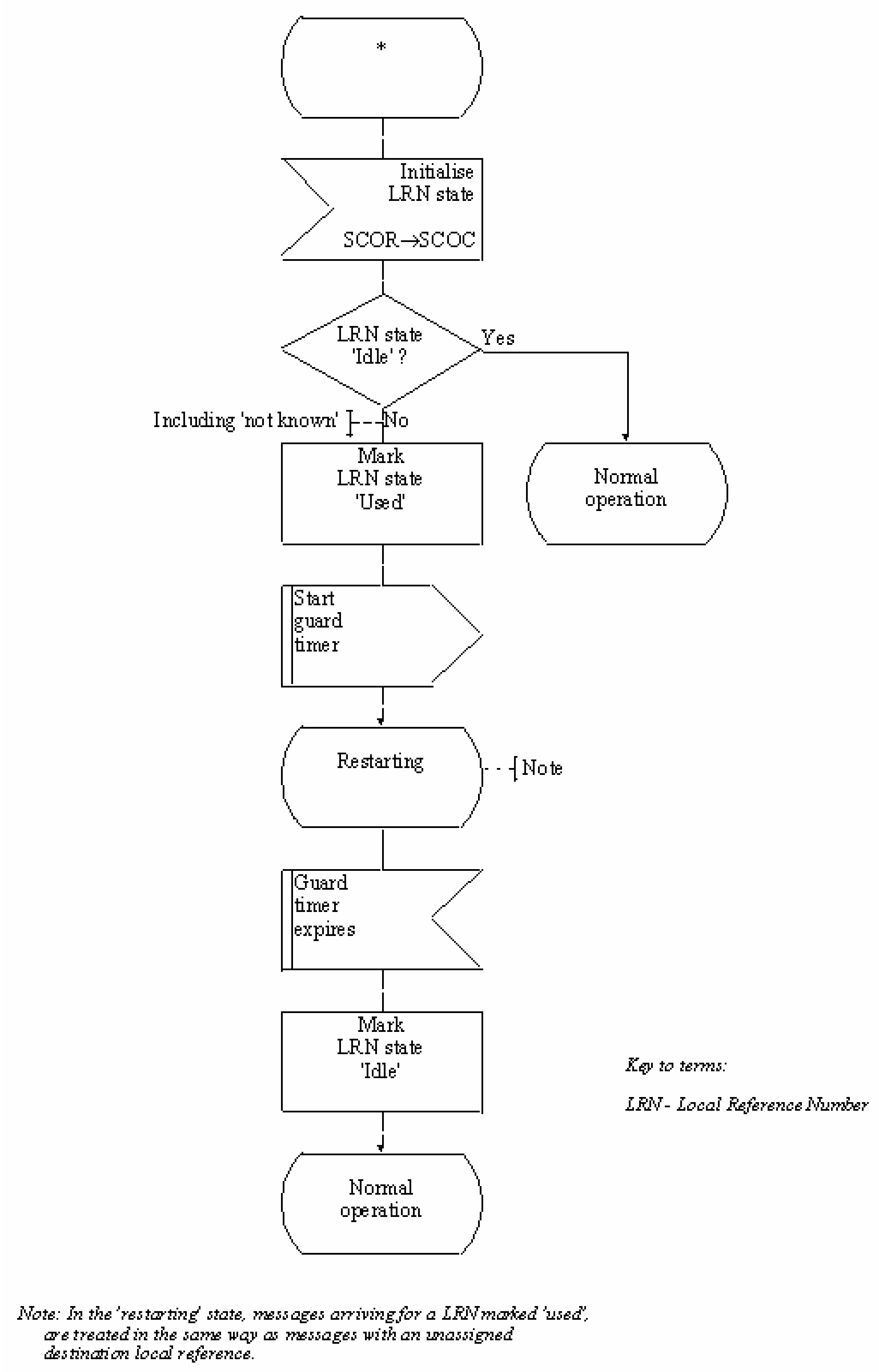


Figure 2J/ATIS-1000112.4 - SCOC, Restart at Recovered Node

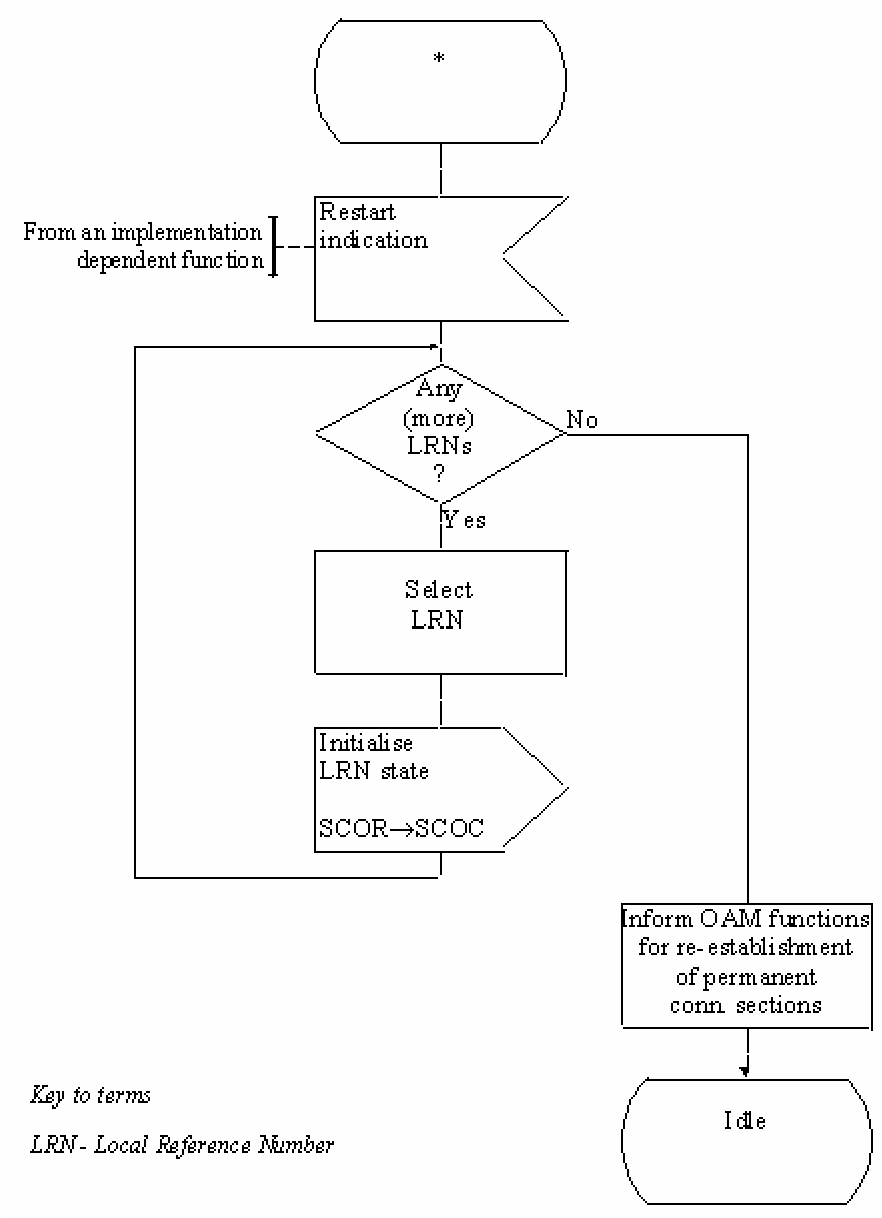


Figure 2K/ATIS-1000112.4 - SCOR, Restart control for SCCP connection-oriented control

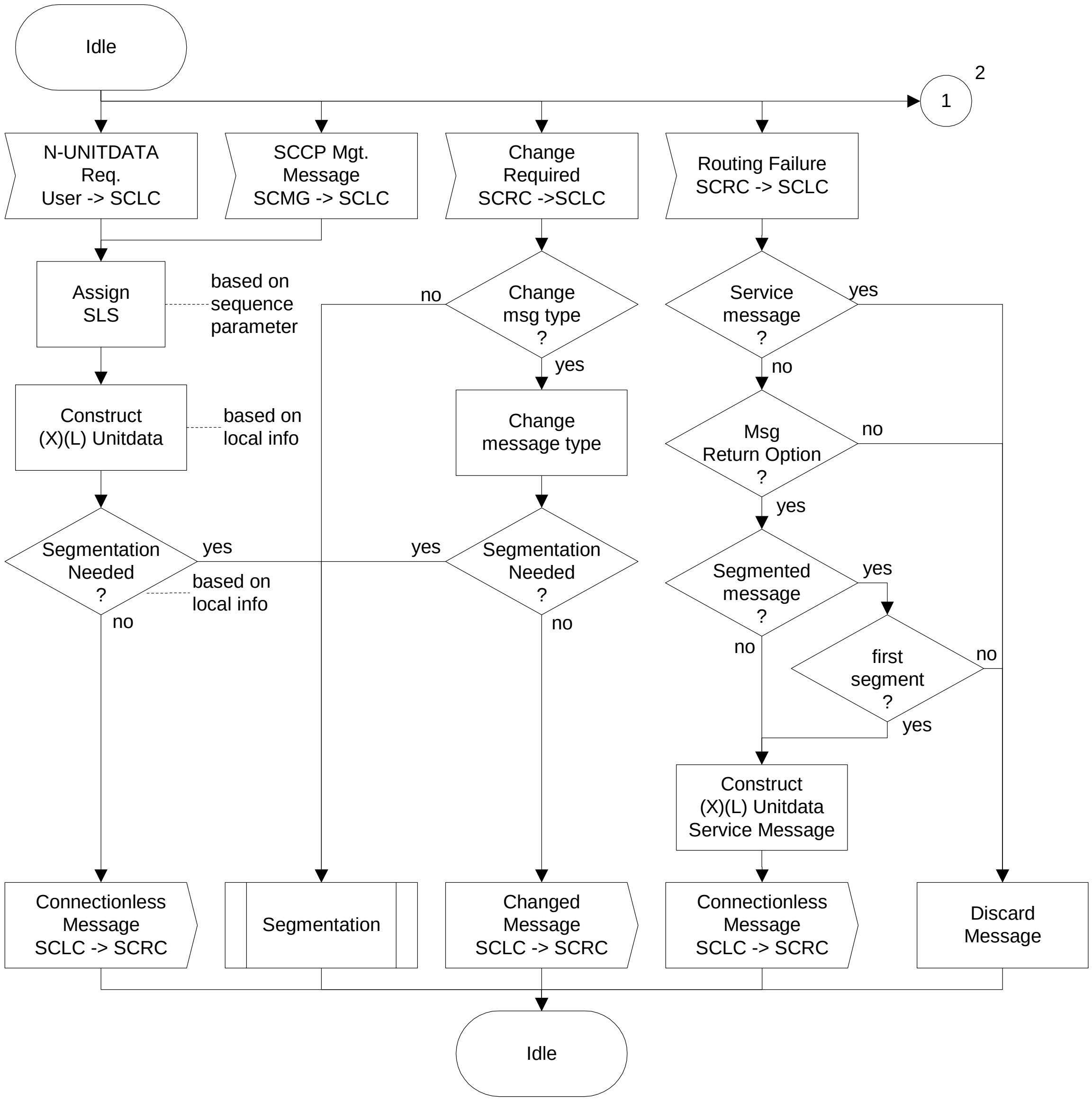


Figure 3/ATIS-1000112.4 - SCCP Connectionless Control (SCLC, Sheet 1 of 2)

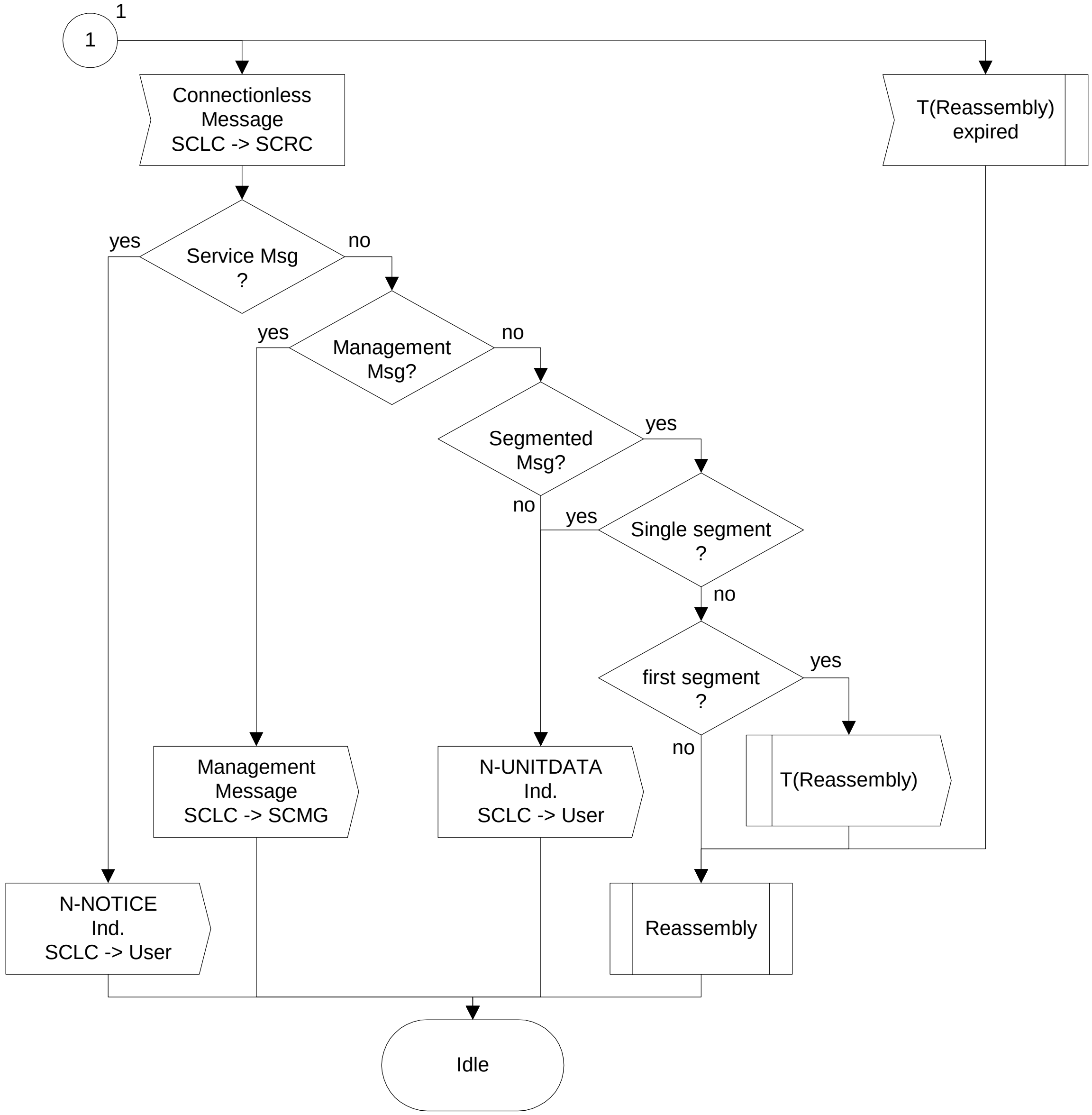


Figure 3/ATIS-1000112.4 - SCCP Connectionless Control (SCLC, Sheet 2 of 2)

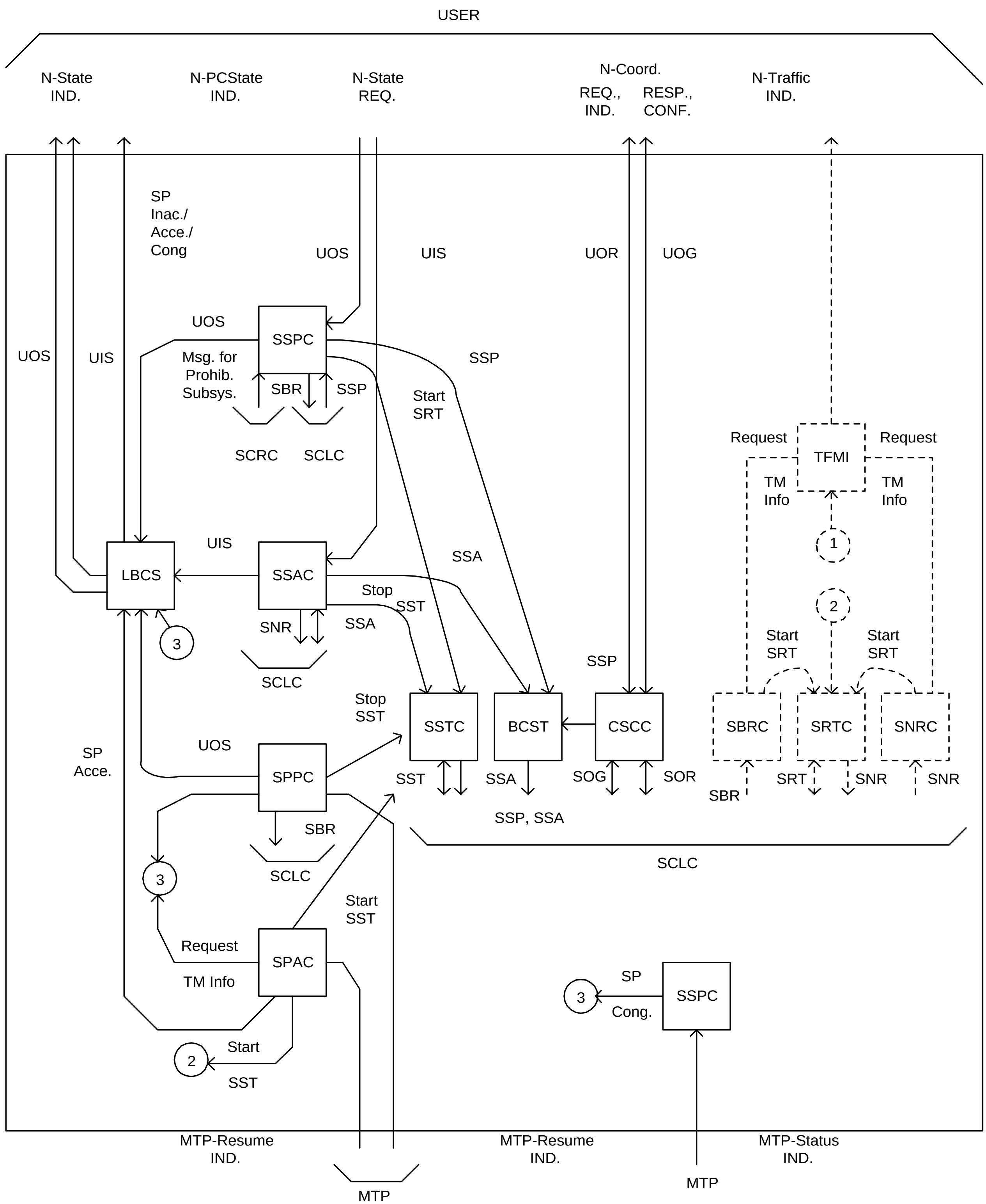


Figure 4/ATIS-1000112.4 - SCCP Management Overview (SCMG)

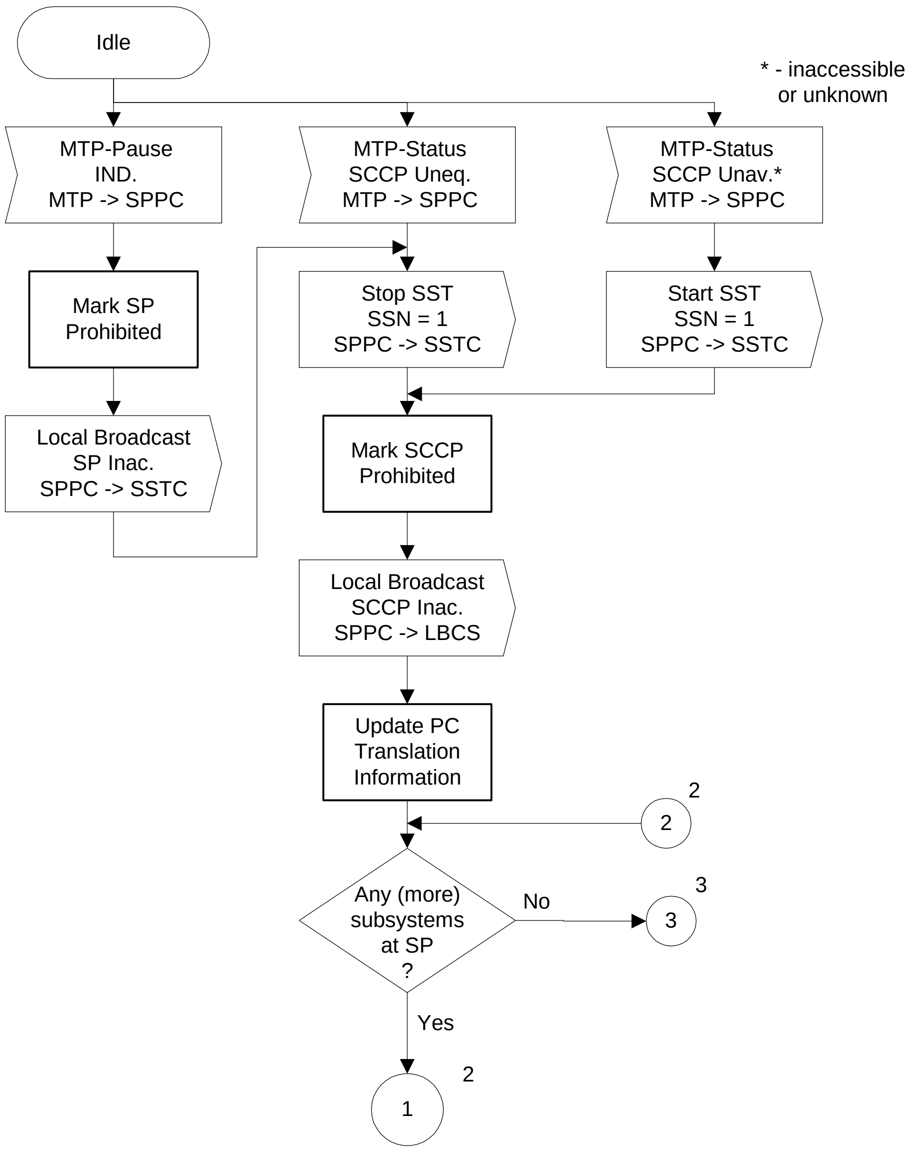


Figure 5/ATIS-1000112.4 - SCCP Management; Signaling Point Prohibited Control (SPPC) (Sheet 1 of 3)

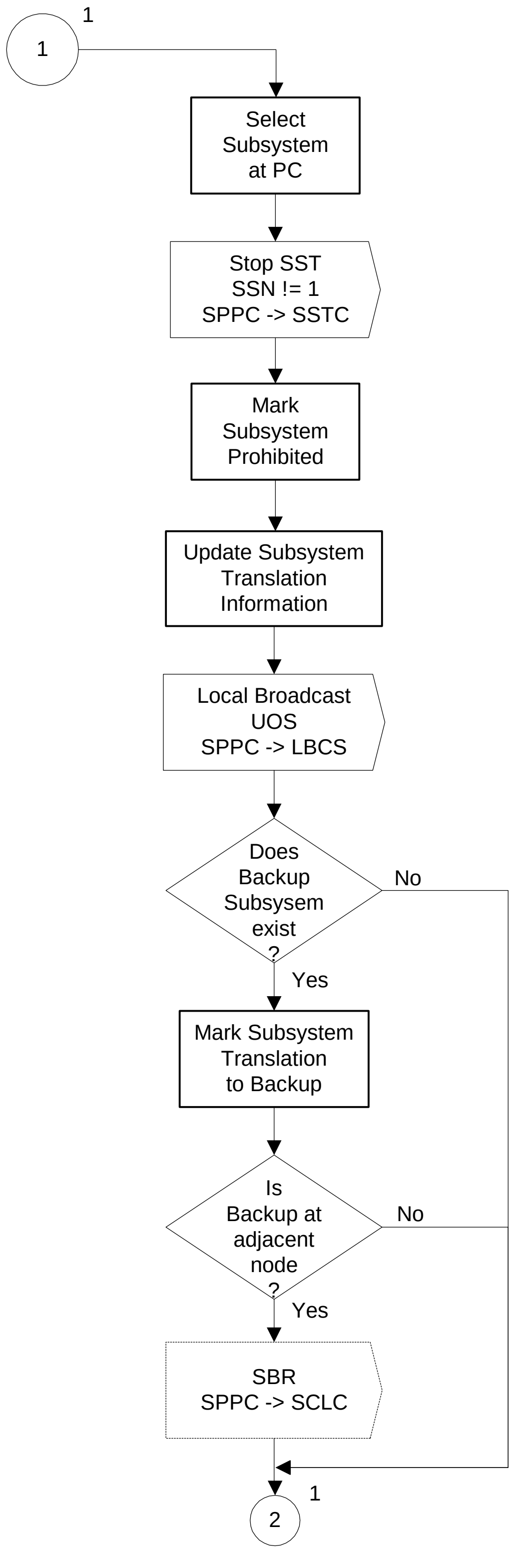


Figure 5/ATIS-1000112.4 - SCCP Management; Signaling Point Prohibited Control (SPPC) (Sheet 2 of 3)

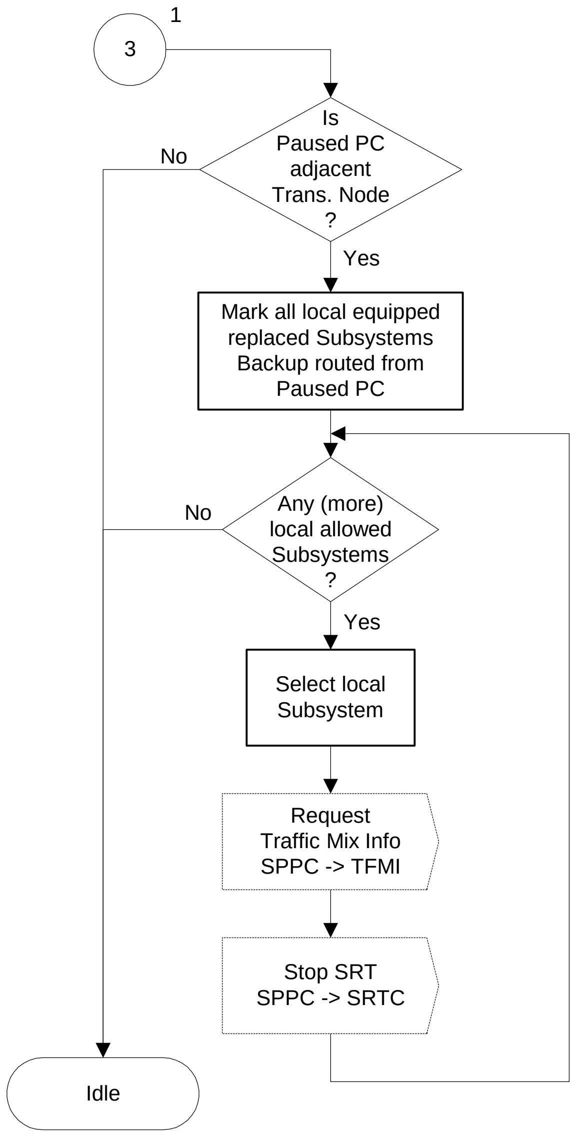


Figure 5/ATIS-1000112.4 - SCCP Management; Signaling Point Prohibited Control (SPPC) (Sheet 3 of 3)

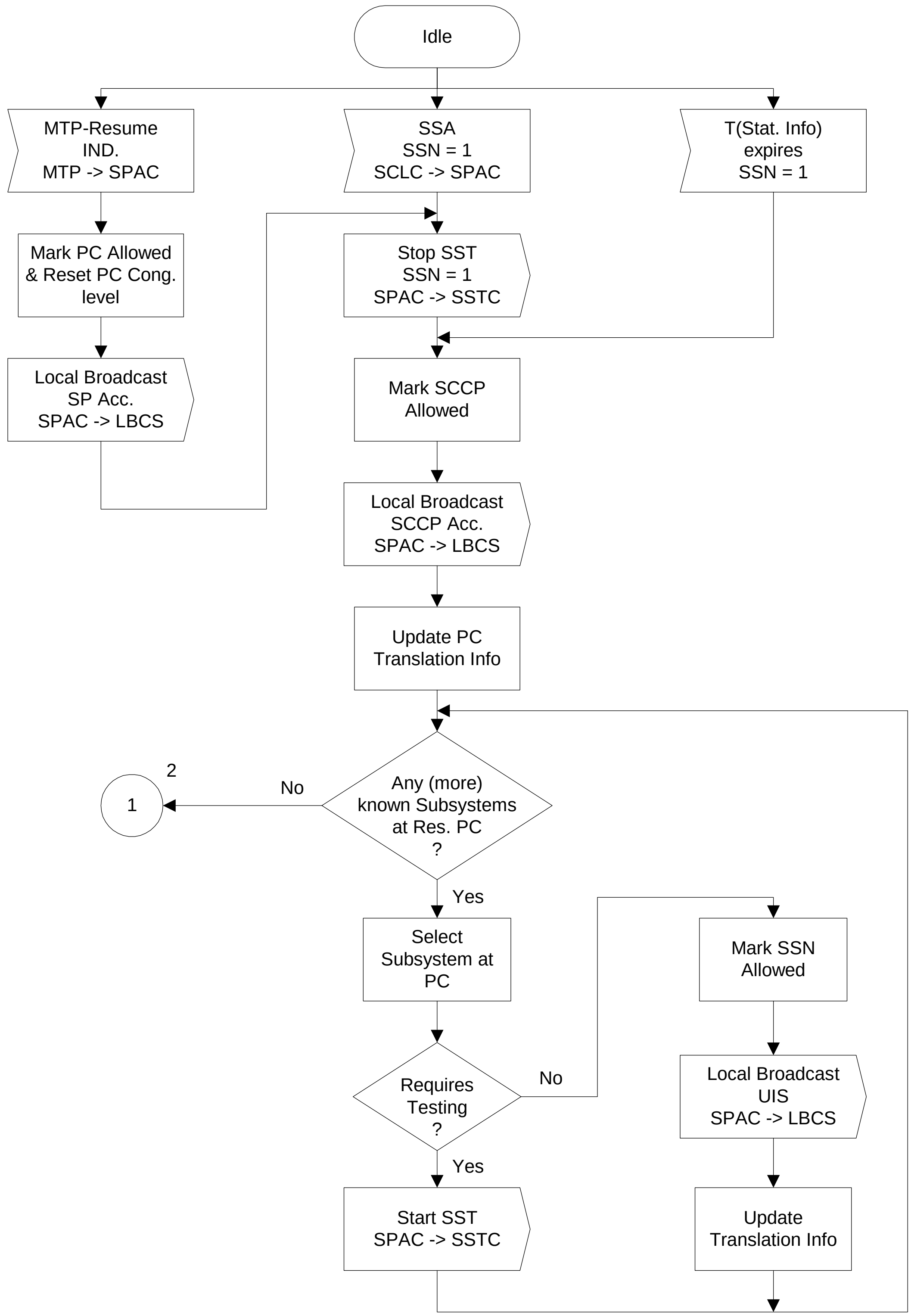


Figure 6/ATIS-1000112.4 - SCCP Management; Signaling Point Allowed Control (SPAC) (Sheet 1 of 2)

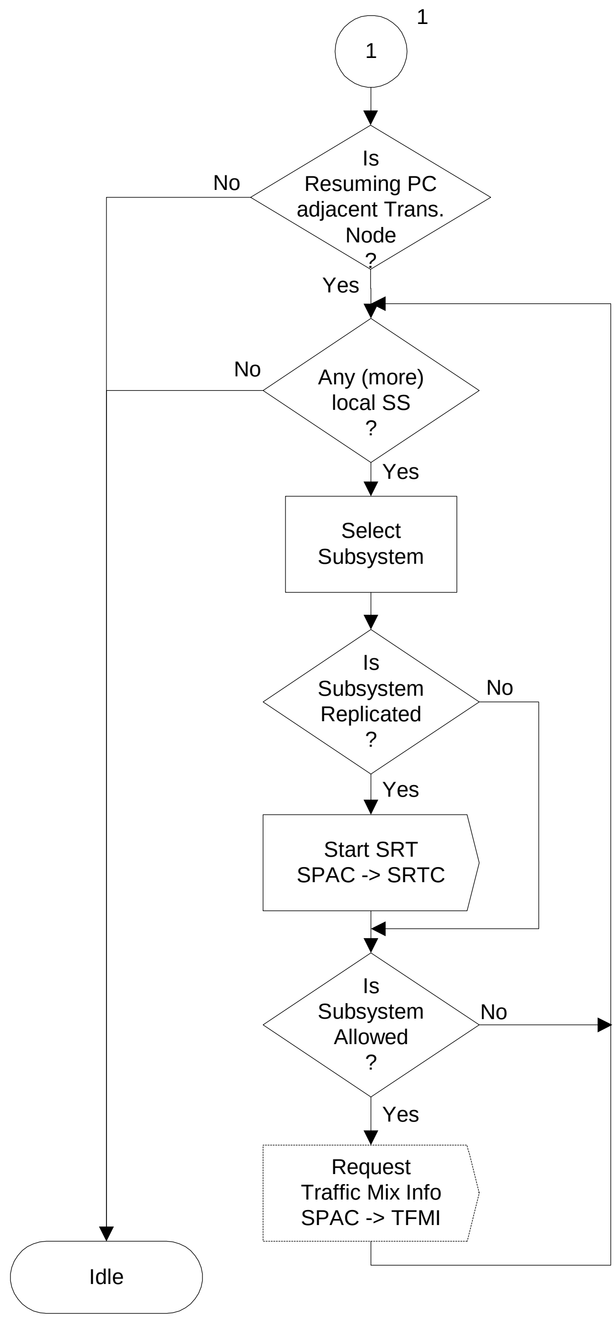


Figure 6/ATIS-1000112.4 - SCCP Management; Signaling Point Allowed Control (SPAC) (Sheet 2 of 2)

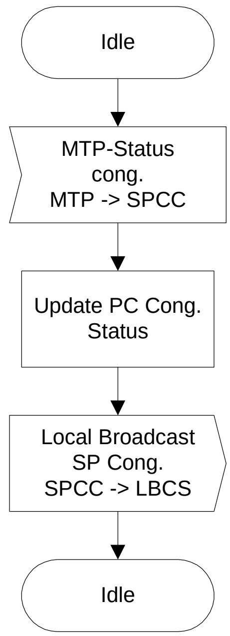


Figure 7/ATIS-1000112.4 - SCCP Management; Signaling Point Congested Control (SPCC)

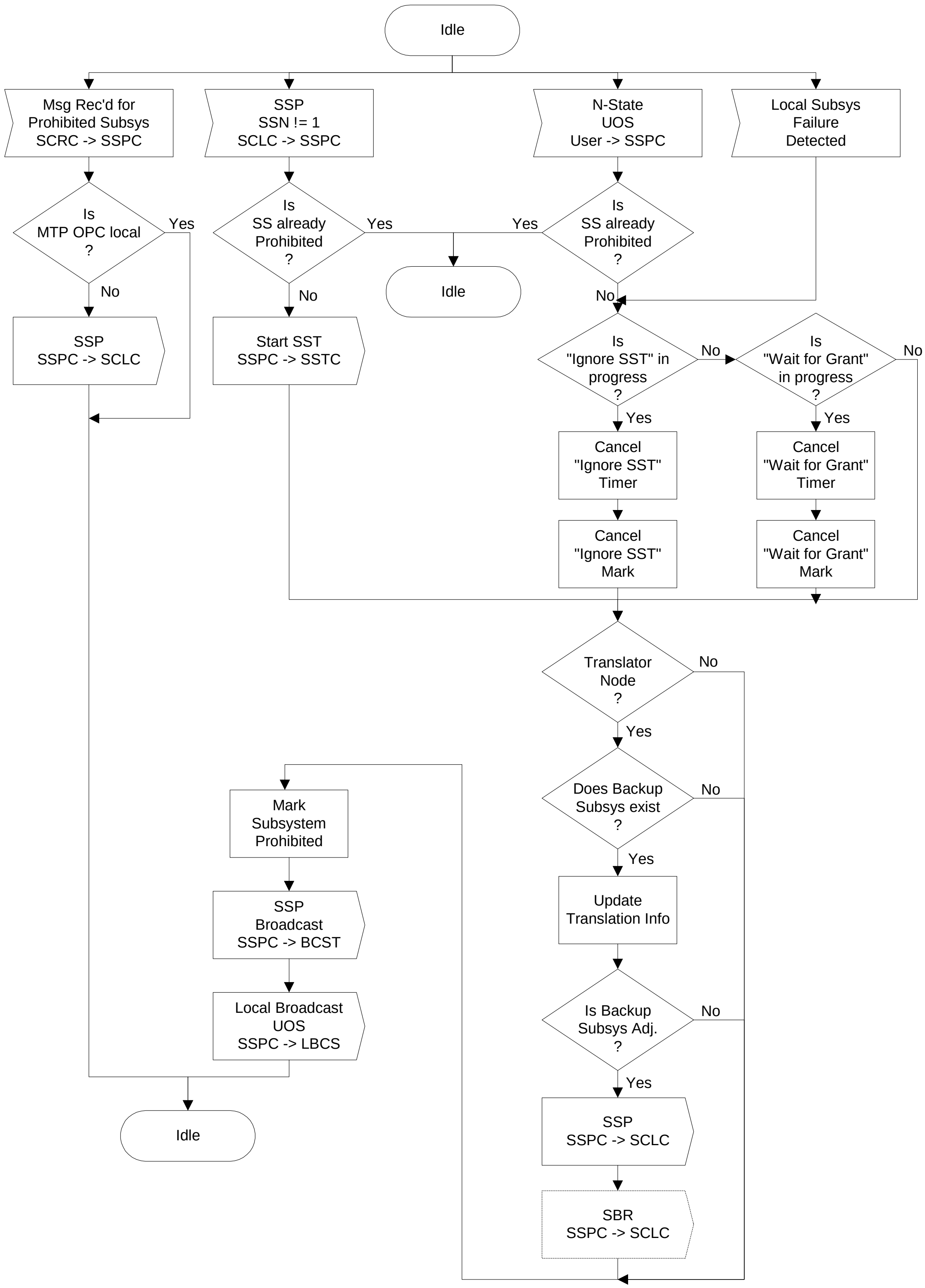


Figure 8/ATIS-1000112.4 - SCCP Management; Subsystem Prohibited Control (SSPC)

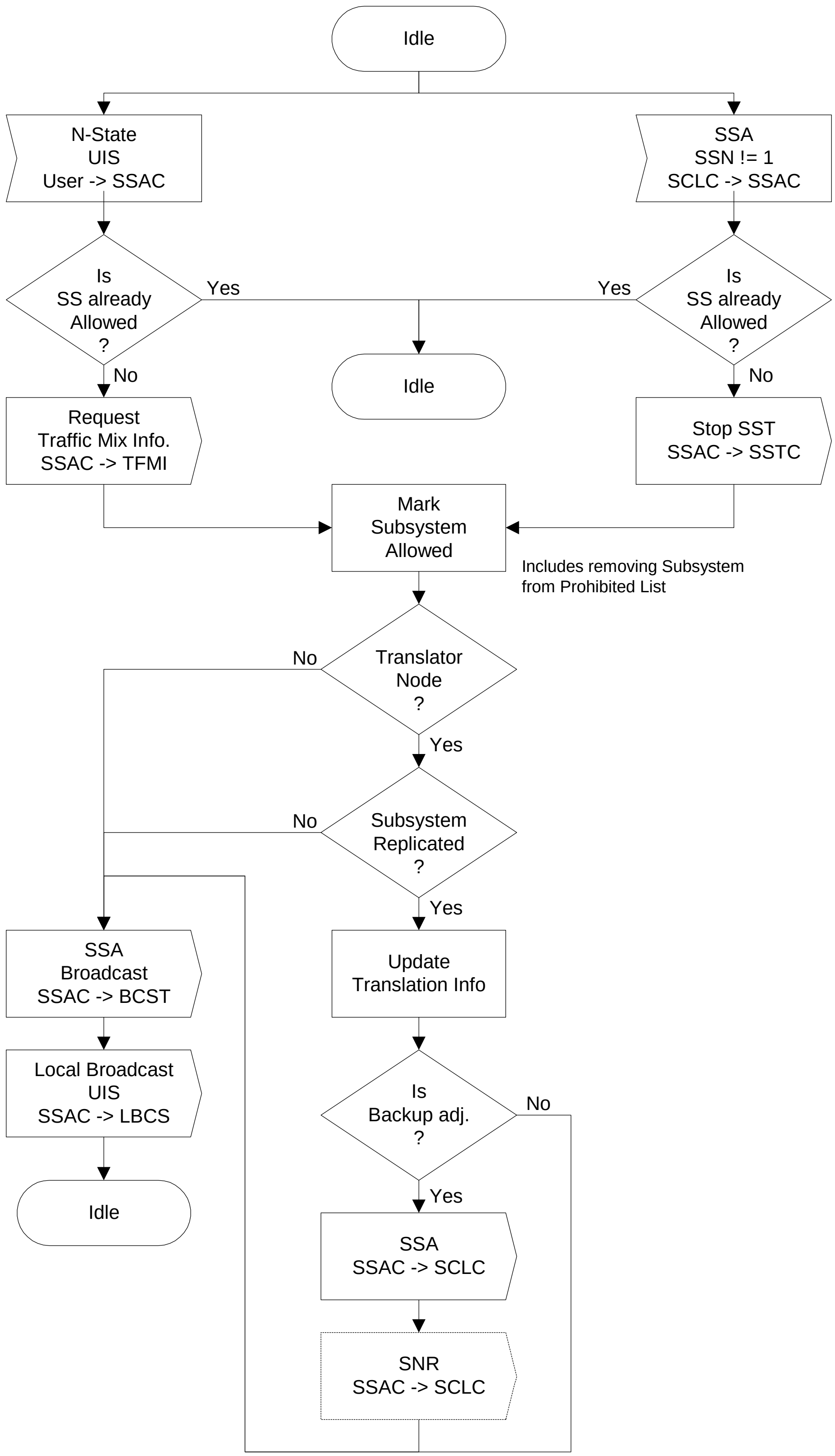


Figure 9/ATIS-1000112.4 - SCCP Management; Subsystem Allowed Control (SSAC)

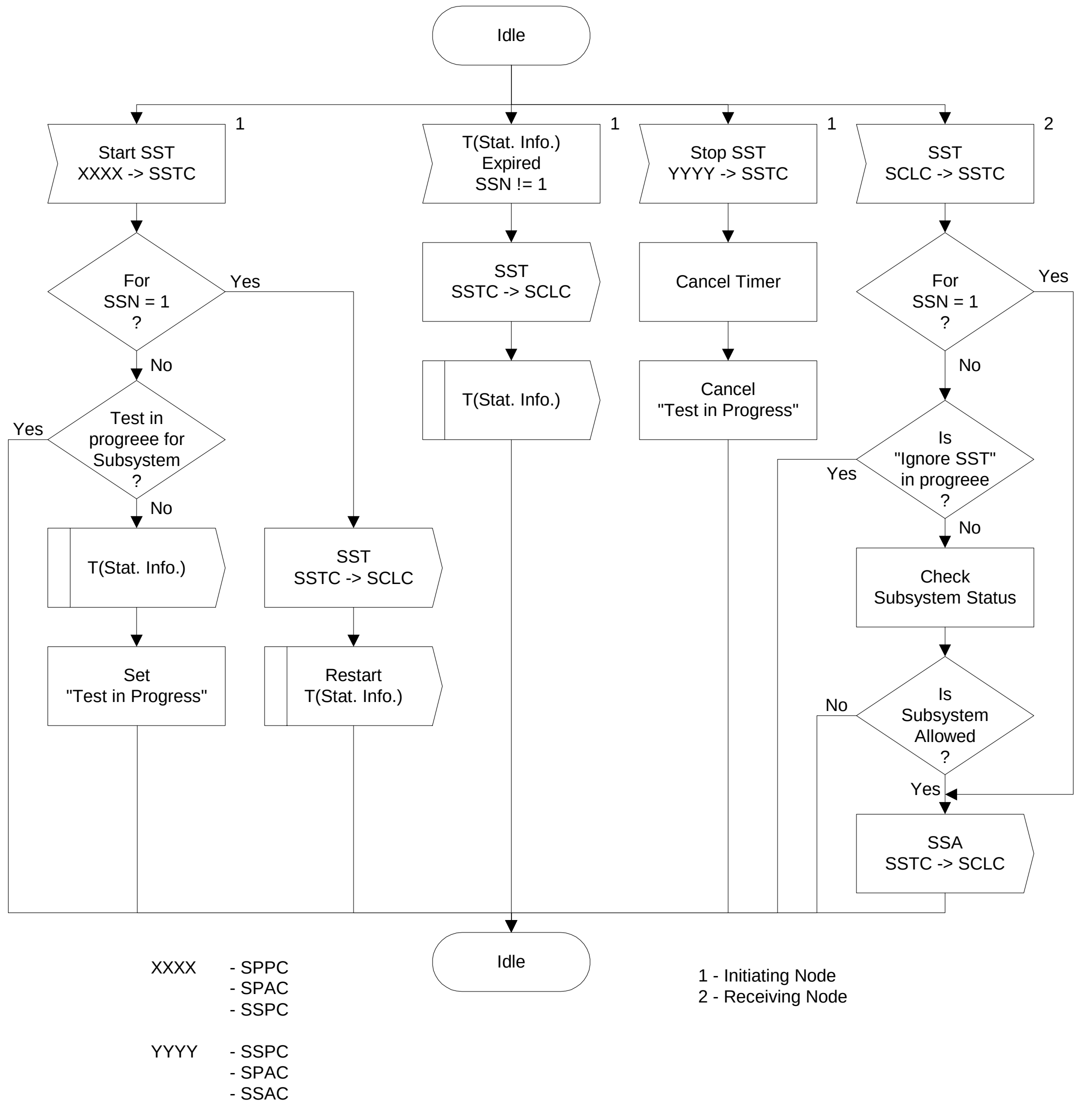


Figure 10/ATIS-1000112.4 - SCCP Management; Subsystem Status Test Control (SSTC)

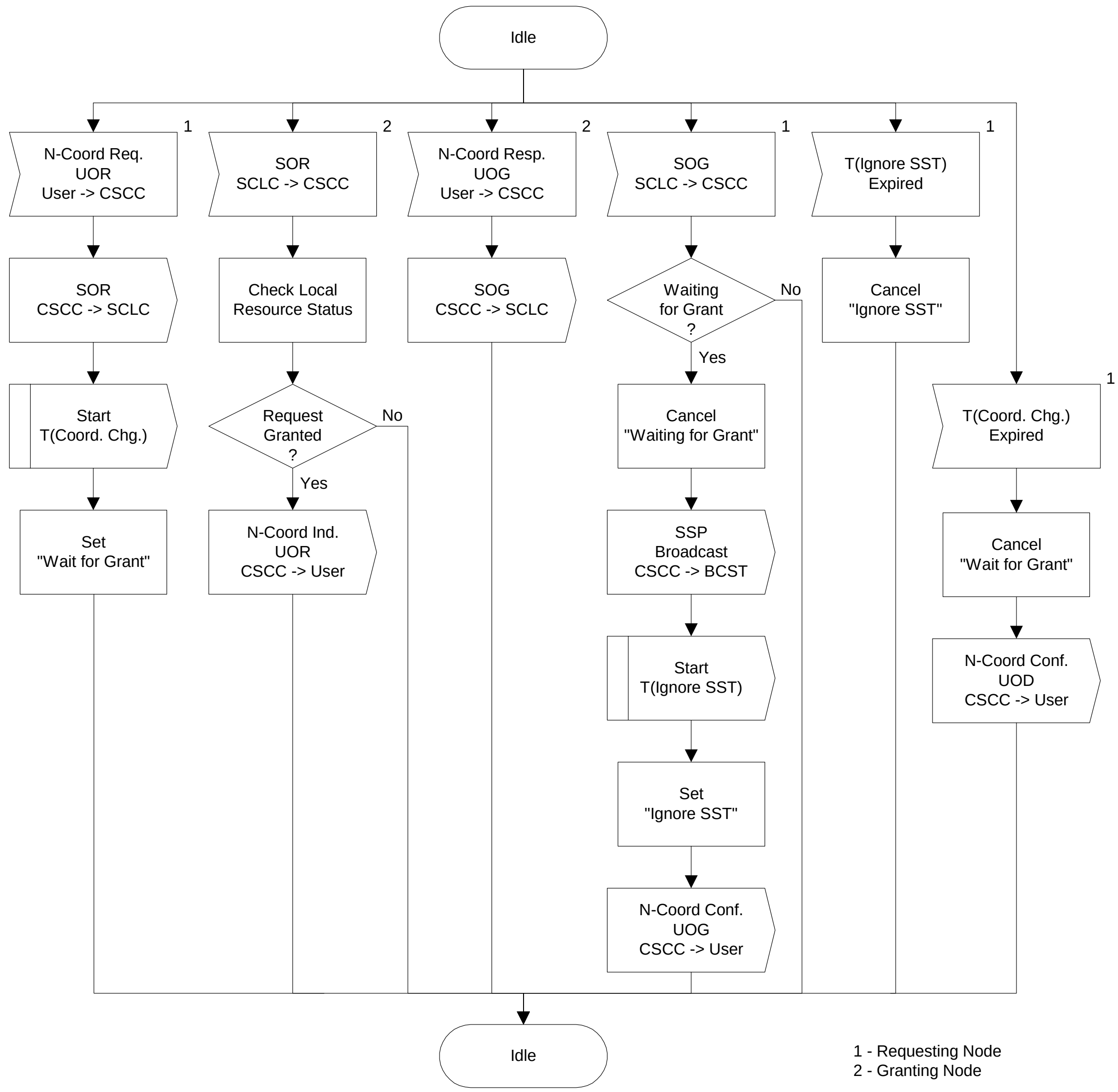


Figure 11/ATIS-1000112.4 - SCCP Management; Coordinated State Change Control (CSCC)

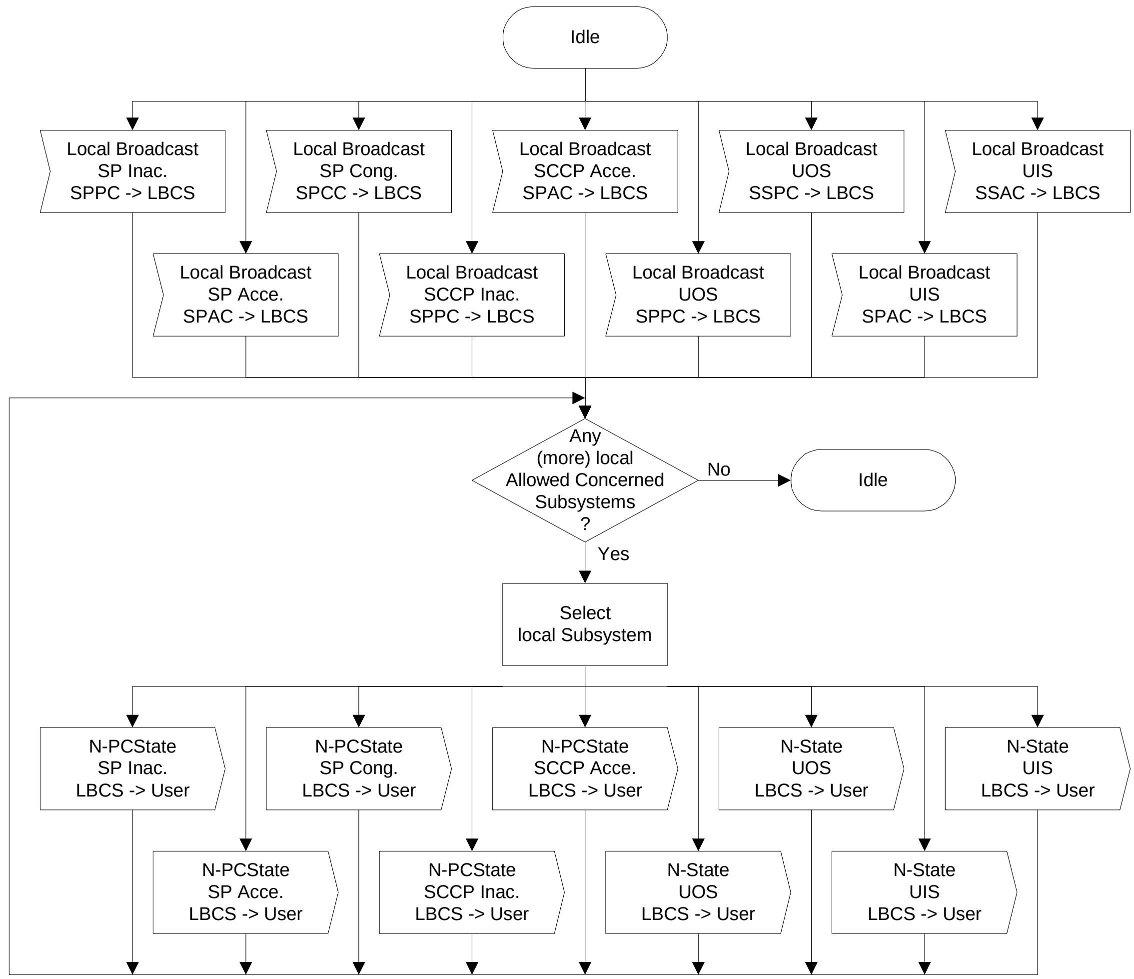


Figure 12/ATIS-1000112.4 - SCCP Management; Local Broadcast (LBCS)

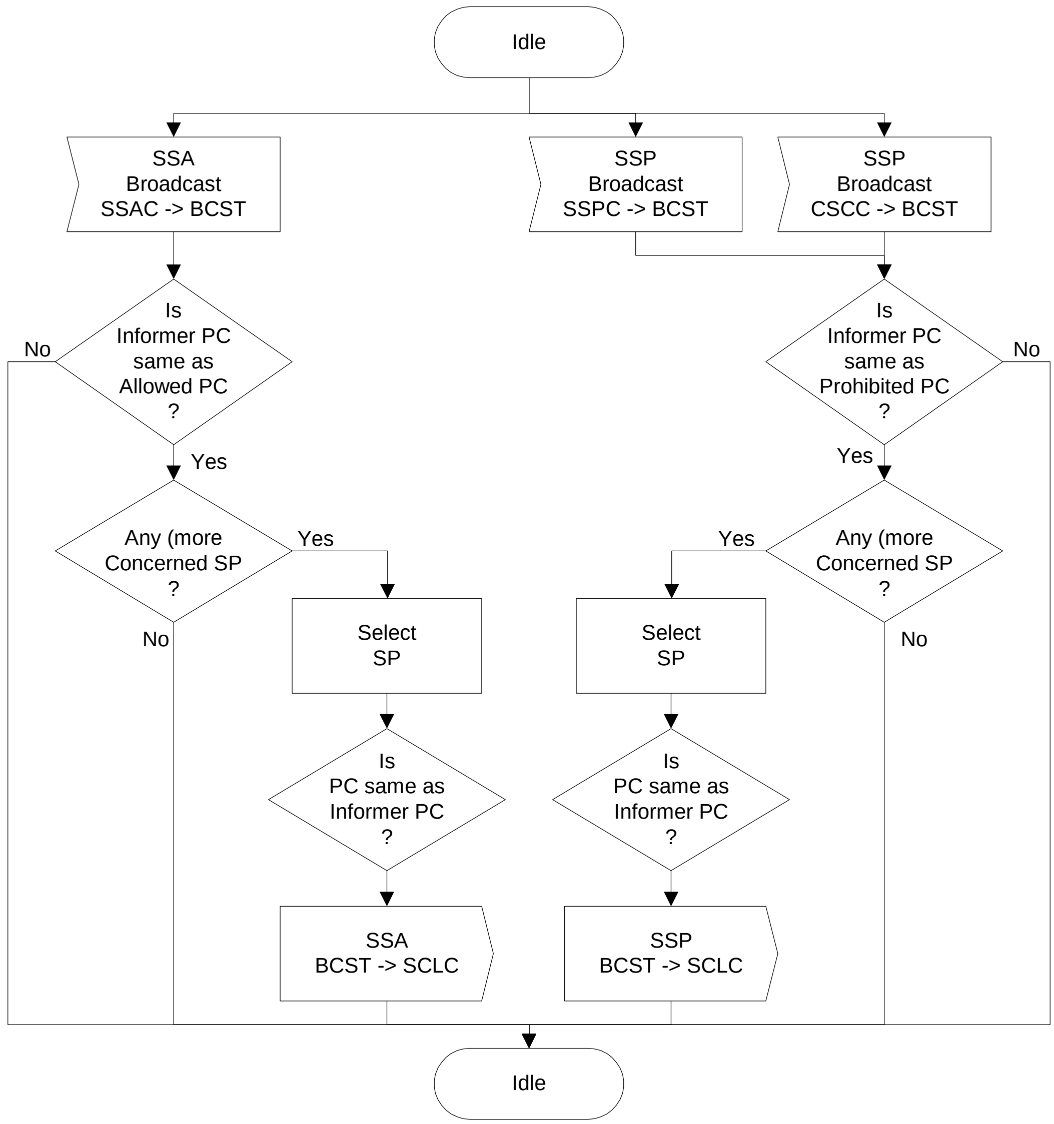


Figure 13/ATIS-1000112.4 - SCCP Management; Broadcast (BCST)

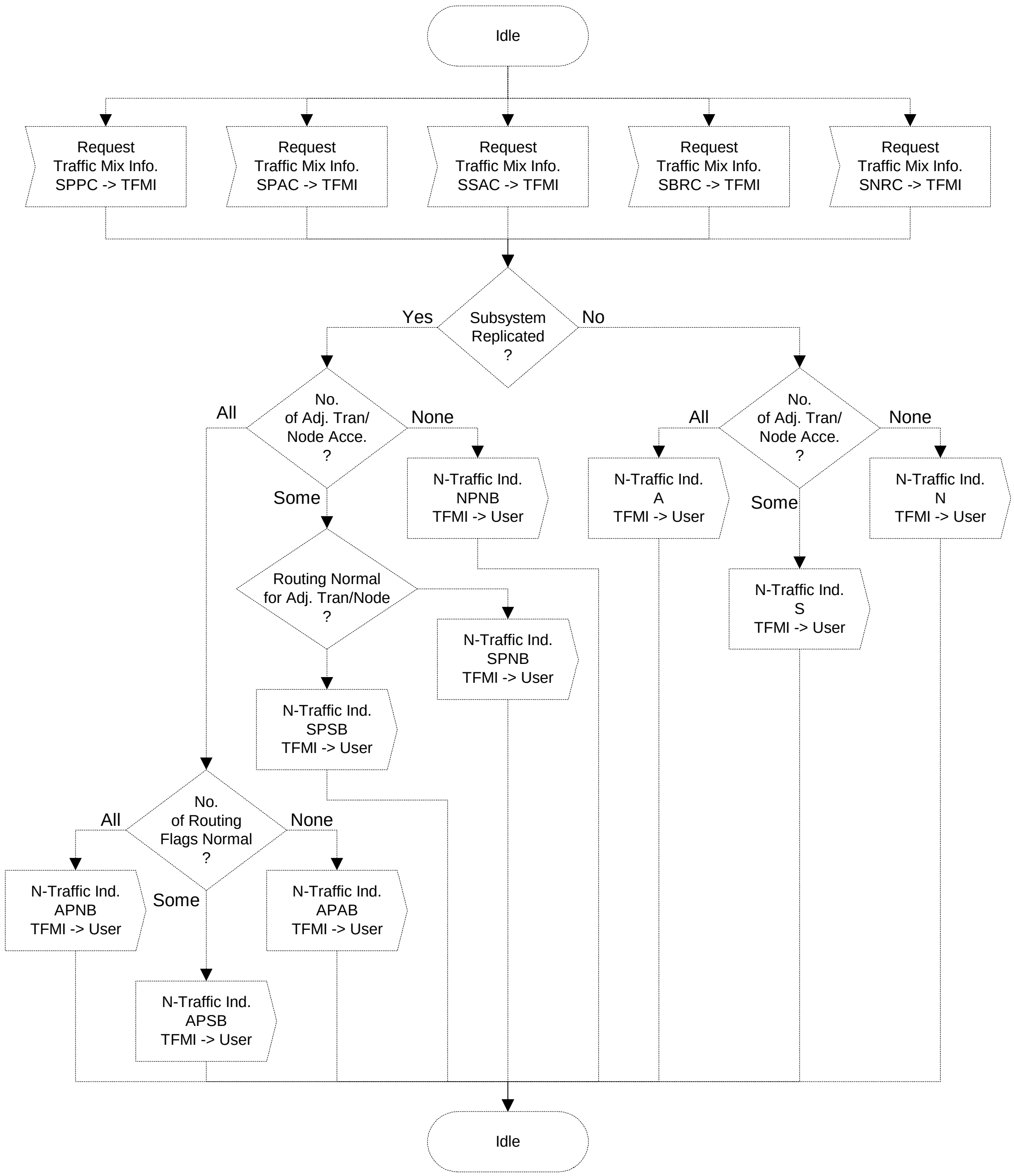


Figure 14/ATIS-1000112.4 - SCCP Management; Traffic Mix Information (TFMI)

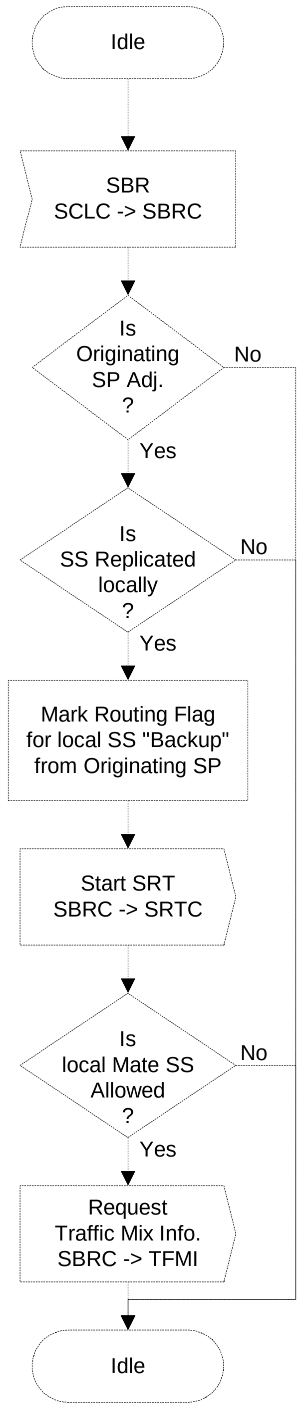


Figure 15/ATIS-1000112.4 - SCCP Management; Subsystem Backup Routing Control (SBRC)

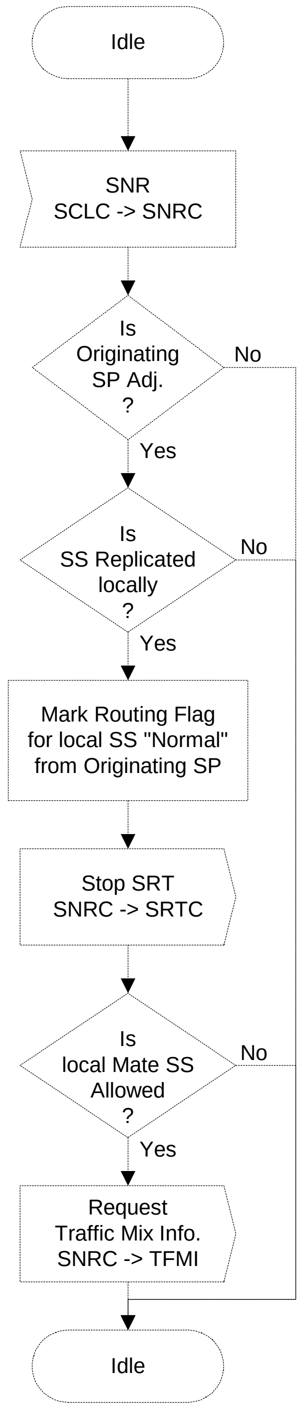


Figure 16/ATIS-1000112.4 - SCCP Management; Subsystem Normal Routing Control (SNRC)

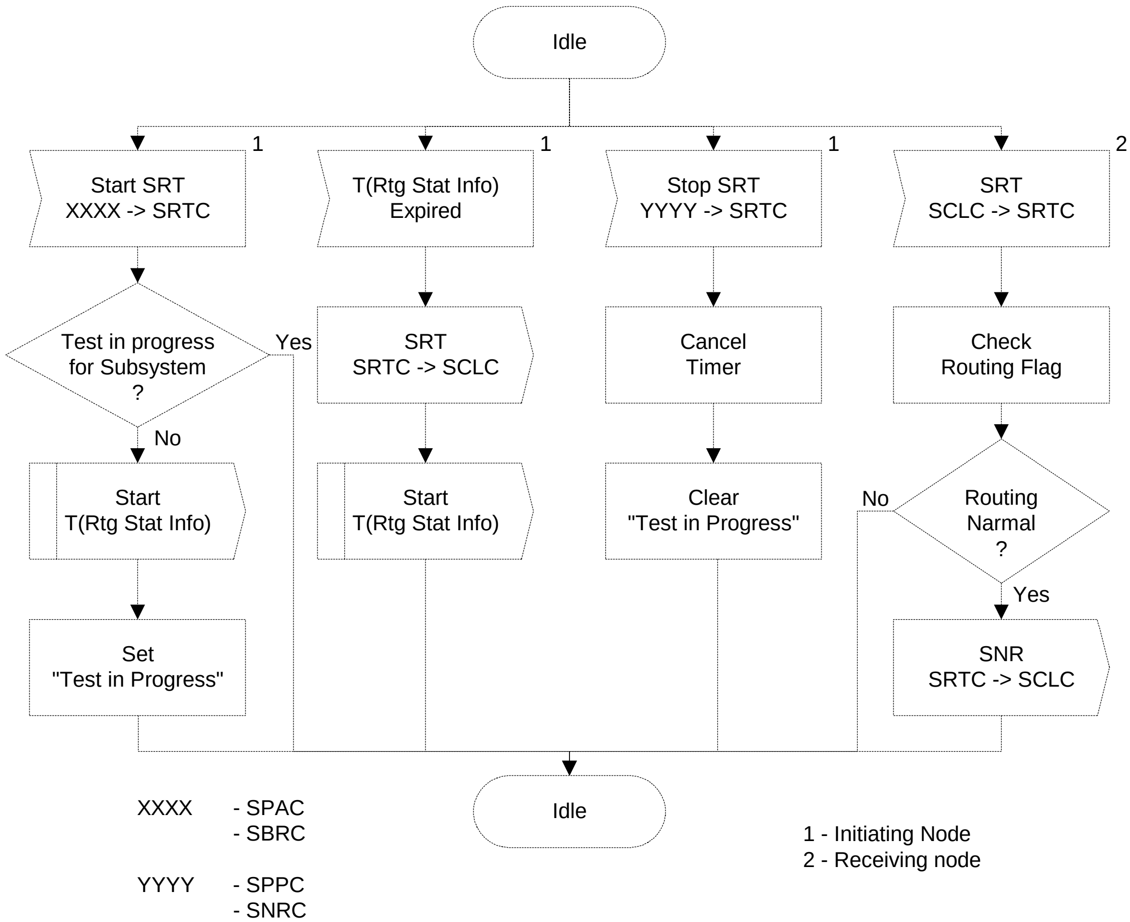


Figure 17/ATIS-1000112.4 - SCCP Management; Subsystem Routing Status Test Control (SRTC)

		Number of Adjacent STPs Accessible	Number of Routing Flags Normal	Traffic Mix
Duplex	I	Both	2	AP/NB
	II	Both	1	AP/SB
	III	Both	0	AP/AB
	IV	One	1	SP/NB
	V	One	0	SP/SB
	VI	Zero	-	NP/NB
Simplex	VII	Both	-	A
	VIII	One	-	S
	IX	Zero	-	N

Figure 18/ATIS-1000112.4 - Architecture Dependent Traffic Mix Calculation

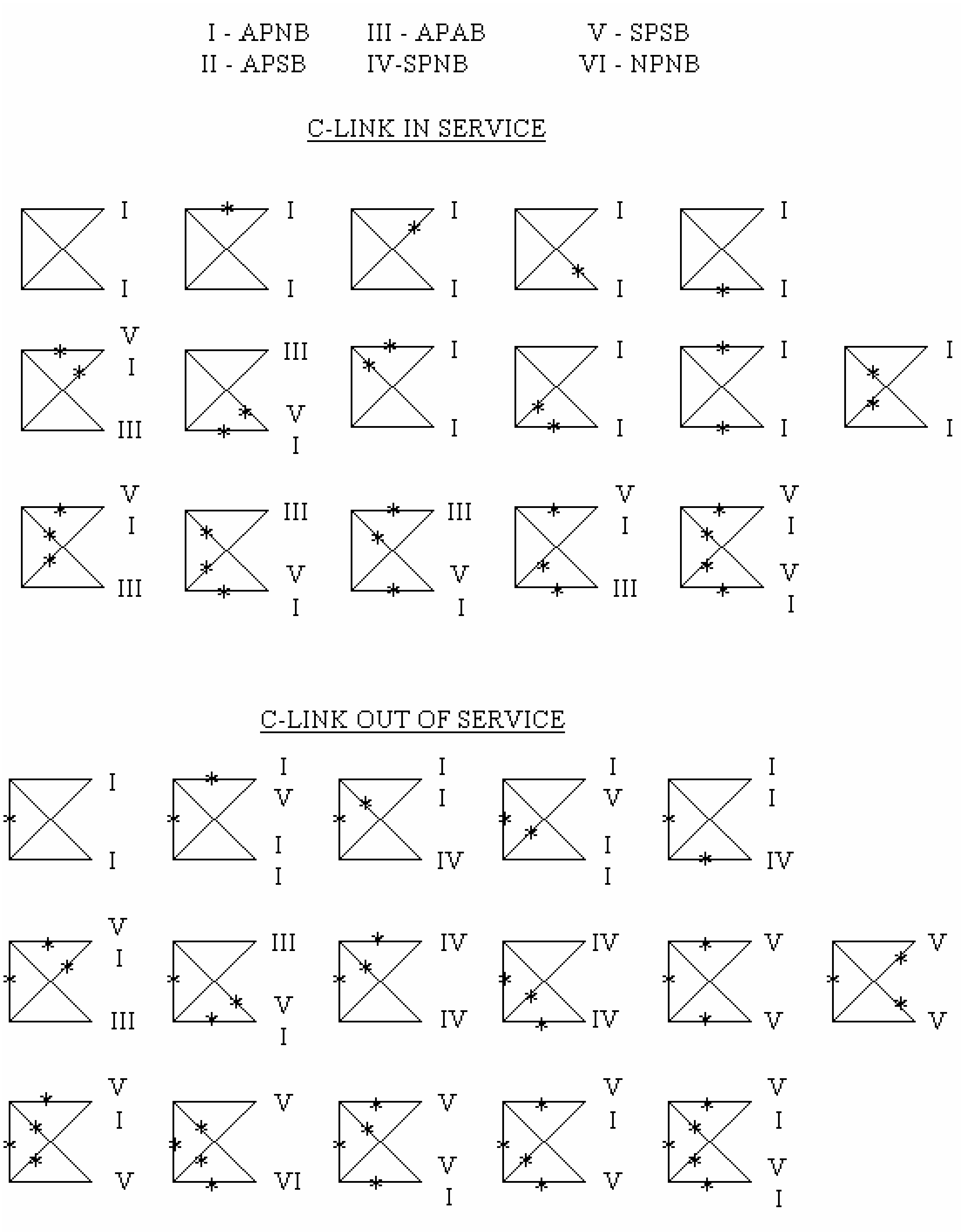


Figure 19/ATIS-1000112.4 - Link Failure Summary

Annex A
(informative)

ANNEX A STATE DIAGRAMS FOR THE SIGNALING CONNECTION CONTROL PART OF SIGNALING SYSTEM NO. 7

A.1 Introduction

This Annex contains the definitions for the symbols used and defines the states of the signaling point X/Y interface and the transitions between states in the normal case.

Annex B contains the full definition of actions, if any, to be taken on the receipt of messages by a signaling point.

A.2 Symbol Definition of the State Diagrams at the Message Interface between Two Nodes (Signaling Points: X and Y)

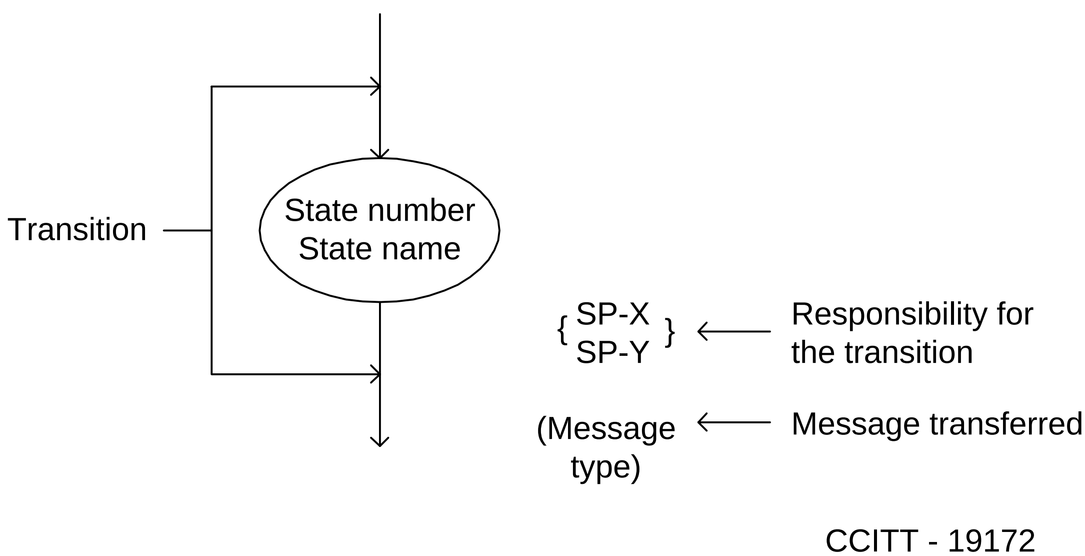


Figure A-1/ATIS-1000112.4 - Symbol Definition of the State Diagram

NOTE 1 - Each state is represented by an ellipse wherein the state name and number are indicated.

NOTE 2 - Each state transition is represented by an arrow. The responsibility for the transition (SP-X or SP-Y) and the message that has been transferred is indicated beside that arrow.

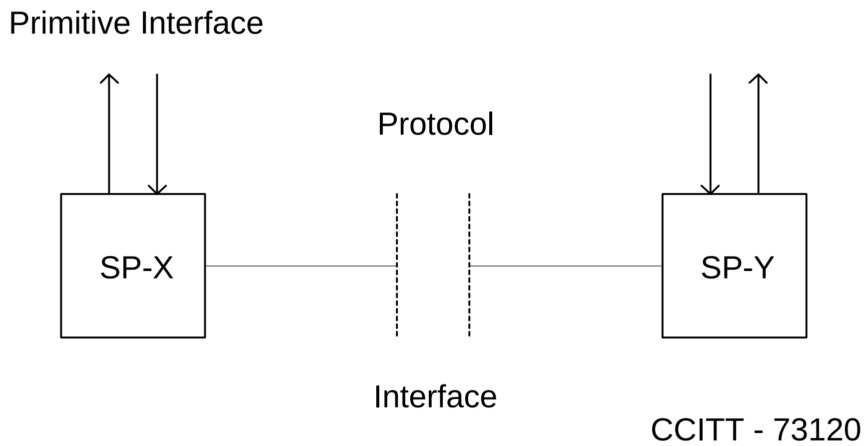


Figure A-2/ATIS-1000112.4 - Primitive and Protocol Interface

NOTE - SP-X and SP-Y are the signaling points X and Y denoting respectively the origin and destination of the connection section concerned.

A.3 Order Definition of the State Diagrams

For the sake of clarity, the normal procedure at the interface is described in a number of small diagrams. In order to describe the normal procedure fully, it is necessary to allocate a priority to the different figures and to relate a higher order diagram with a lower one. This has been done by the following means:

- The figures are arranged in order of priority with Figure A-3/ATIS-1000112.4 (connection establishment) having the highest priority and subsequent figures having lower priority. Priority means that when a message belonging to a higher order diagram is transferred, that diagram is applicable, and the lower order one is not.
- The relation with a state in a lower order diagram is given by including that state inside an ellipse in the higher order diagram.
- The message abbreviations are those defined in Chapter ATIS-1000112.2.

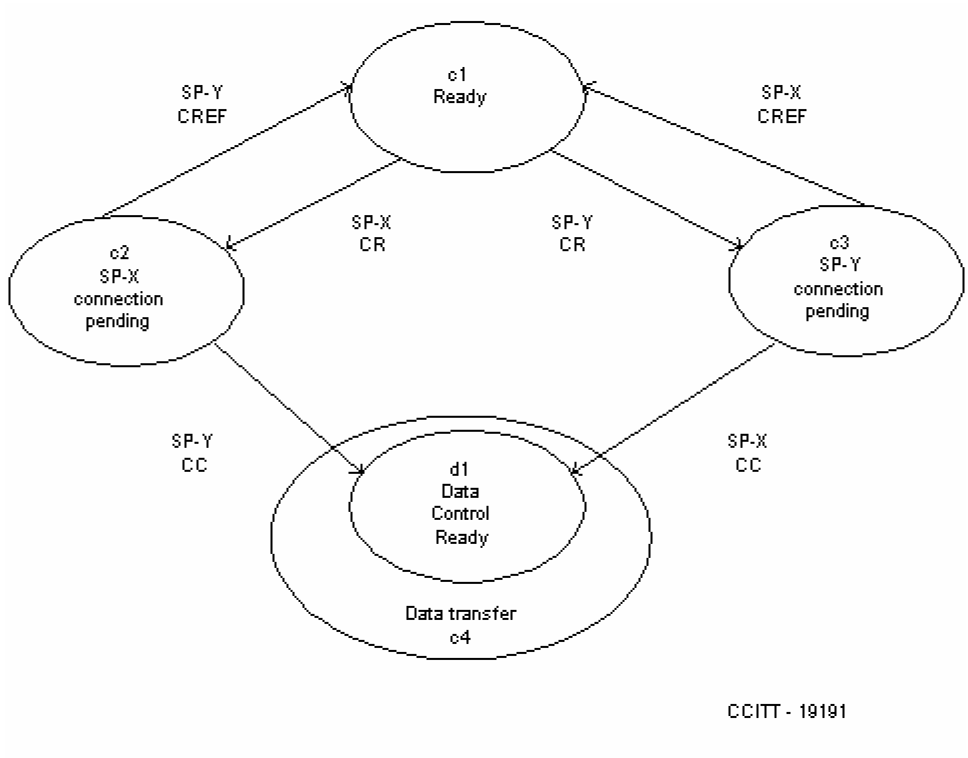


Figure A-3/ATIS-1000112.4 - State Transition Diagram for Sequences of Messages during Connection Establishment

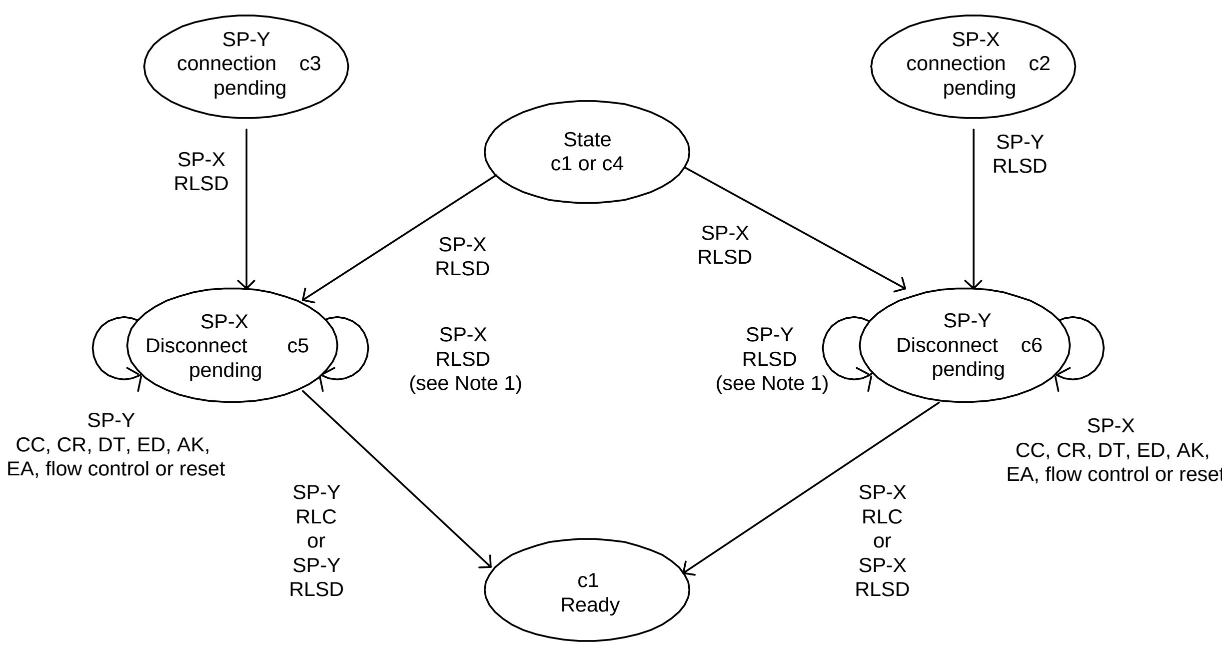


Figure A-4/ATIS-1000112.4 - State Transition Diagram for Sequence of Messages during Connection Release

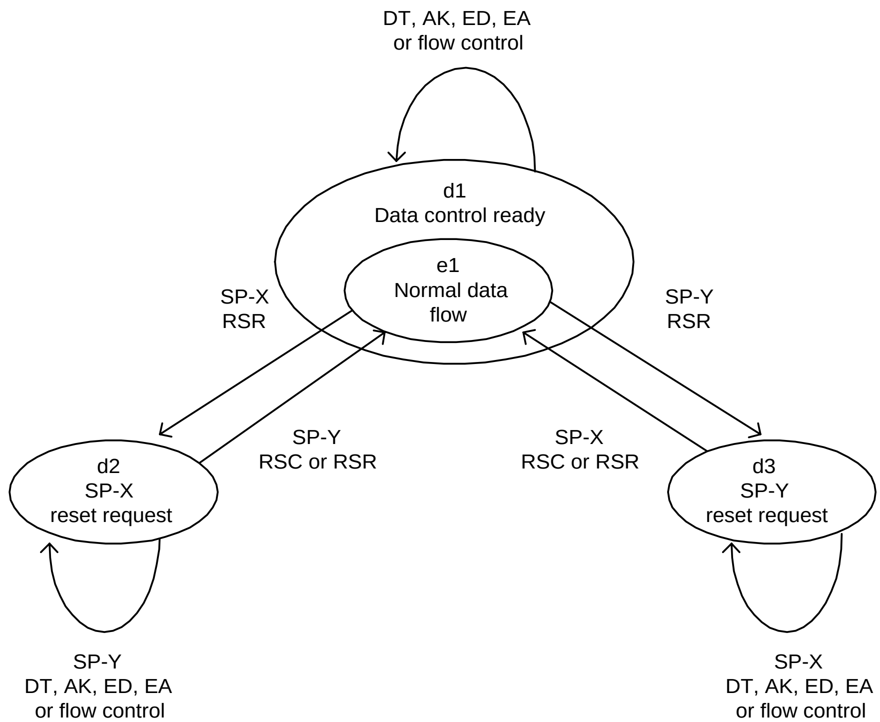


Figure A-5/ATIS-1000112.4- State Transition Diagram for the Transfer of Reset Messages within the Data Transfer (c4) State

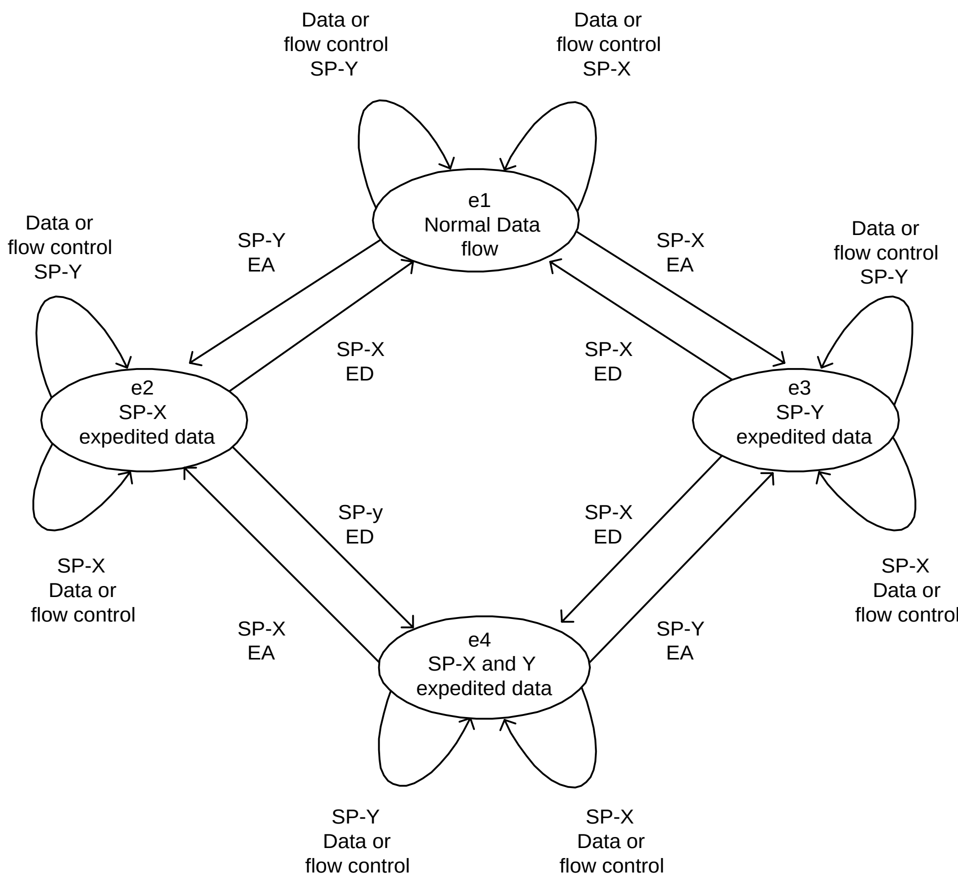


Figure A-6/ATIS-1000112.4 - State Transition Diagram for the Transfer of Data, Expedited Data, and Flow Control within the Data Transfer (c4) State

Annex B
(informative)

ANNEX B ACTION TABLES FOR THE SIGNALING CONNECTION CONTROL PART (SCCP) OF SIGNALING SYSTEM NO. 7

B.1 Introduction

This Annex contains the definitions for the symbols used and contains the full definition of actions, if any, to be taken on the receipt of messages by a signaling point (node).

Annex A contains the full definition of states of the signaling point X/Y interface and the transitions between states in the normal case.

B.2 Symbol Definition of the Action Tables

The entries given in Tables B-1 and B-2/ATIS-1000112.4 indicate the action, if any, to be taken by a SP on receipt of any kind of message, and the state the SP enters, which is given in parentheses, following the action taken.

The restart procedure actions tables are for further study and are not included.

In any state it is possible to receive an Error message (ERR). The reaction, if any, depends on the contents (error cause and possible diagnostics) of the message and is for further study.

The reaction on messages received with procedure errors (e.g., too long, invalid P(R), not octet aligned, etc.) are normal actions and will be described in the text. So they are covered by the actions indicated as NORMAL.

B.3 Table of Contents

- Table B-1/ATIS-1000112.4: Actions taken by SP-Y on receipt of messages.
- Table B-2/ATIS-1000112.4: Actions taken by SP-Y on receipt of messages with known message type and containing mismatch information.
- Table B-3/ATIS-1000112.4: Actions taken by SP-Y on receipt of messages during connection establishment and release phases.
- Table B-4/ATIS-1000112.4: Actions taken by SP-Y on receipt of messages during the data transfer phase in a given state: reset.
- Table B-5/ATIS-1000112.4: Actions taken by SP-Y on receipt of messages during the data transfer phase in a given state: data, expedited data, flow control.

Table B-1/ATIS-1000112.4 - Action taken by SP-Y on receipt of messages

State of the interface as perceived by node SP-Y Message received by node SP-Y	Any state
Any message with message length shorter than n octets (n = for further study)	DISCARD
Any message with unknown message type	DISCARD
Any message with known message type and: a) unassigned destination local reference number; or b) Originating Point Code not equal to the remote PC (if known); or c) source local reference number not equal to the remote local reference number (if known)	see Table B-2/ATIS-1000112.4
Any other message	see Table B-3/ATIS-1000112.4

Legend for Table B-1/ATIS-1000112.4

DISCARD: SP-Y discards the received message and takes no subsequent action.

Table B-2/ATIS-1000112.4 - Action Taken by SP-Y on Receipt of Messages with Known Message Type and Containing Mismatch Information as in Table B-1/ATIS-1000112.4

State of the interface as perceived by node SP-Y Message received by node SP-Y	Any state
RLSD (Y, X)	RLC (X, Y)
Any message without source local reference	DISCARD
RLC (Y, X)	DISCARD
Other messages with both references (Y, X)	ERR (X, -)

Legend for Table B-2/ATIS-1000112.4

DISCARD: SP-Y discards the received message and takes no subsequent action.

NAME (d, s) : NAME = abbreviation of message

d = destination reference number

s = source reference number

Table B-3/ATIS-1000112.4 - Action Taken by SP-Y on Receipt of Messages During Connection Establishment and Release Phases

State of the interface as perceived by node SP-Y / Message received by node SP-Y	Signaling Connection Control ready : r1					
	Ready (c1)	SP-X connection pending (c2)	SP-Y connection pending (c3)	Data transfer (c4)	SP-X disconnect pending (c5)	SP-Y disconnect pending (c6)
Connection Request (CR)	NORMAL (c2)	see Note 1				
Connection Confirm (CC)	see Table B-2/ATIS-1000112.4	ERROR (c6)	NORMAL (c4)	ERROR (c6)	ERROR (c6)	DISCARD (c6)
Connection Refused (CREF)		ERROR (c6)	NORMAL (c1)	ERROR (c6)	ERROR (c6)	ERROR (c6)
Released (RLSD)		ERROR (c6)	NORMAL (c5)	NORMAL (c5)	DISCARD (c5)	NORMAL (c1)
Released complete (RLC)		ERROR (c6)	ERROR (c6)	ERROR (c6)	ERROR (c6)	NORMAL (c1)
Other messages		ERROR (c6)	ERROR (c6/c1) See Note 2	see Table B-4/ATIS-1000112.4	ERROR (c6)	DISCARD (c6)

Legend for Table B-3/ATIS-1000112.4

NORMAL: The action taken by SP-Y follows the normal procedures as defined in the appropriate sections of the procedure text.

DISCARD: SP-Y discards the received message and takes no subsequent action.

ERROR: SP-Y discards the received message and initiates a connection release by sending a RLSD message with proper invalid type cause.

NOTE 1 -Reception of CR in these states is not possible because CR does not contain a destination local reference number (no search is performed).

NOTE 2 - Release can only be performed if the message contains a source local reference number.

Table B-4/ATIS-1000112.4 - Action Taken by Node SP-Y on Receipt of Messages During the Data Transfer State

State of the interface as perceived by node SP-Y / Message received by node SP-Y	Data transfer : C4		
	Data control Ready (d1)	SP-X reset request (d2)	SP-Y reset request (d3)
Reset Request (RSR)	NORMAL (d2)	DISCARD (d2)	NORMAL (d1)L
Reset Confirmation (RSC)	ERROR (d3)	ERROR (d3)	NORMAL (d1)
Other messages	see Table B-5/ATIS-1000112.4	ERROR (d3) Note 1	DISCARD (d3) Note 2

Legend for Table B-4/ATIS-1000112.4

NORMAL: The action taken by SP-Y follows the normal procedures as defined in the appropriate sections of the procedure text.

DISCARD: Signaling point Y discards the received message and takes no subsequent action.

ERROR: Signaling point Y discards the received message and initiates reset by transmitting a RSR message with the appropriate cause indication.

NOTE 1 - If signaling point Y issues a RSR message as a result of an error condition in state d2, it should eventually consider the interface to be in the Data Control Ready State (d1).

NOTE 2 - Messages received exceeding the maximum permitted length will invoke the ERROR procedure.

Table B-5/ATIS-1000112.4 - Actions Taken by SP-Y on Receipt of Messages During the Data Control Ready State

State of the interface as perceived by node SP-Y / Message received by node SP-Y	Data control ready : d1			
	Normal data flow (c1)	SP-X expedited data (c2)	SP-Y expedited data (c3)	SP-X and SP-Y expedited data (c4)
Expedited Data (ED)	NORMAL (c2)	ERROR (d3)	NORMAL (c4)	ERROR (d3)
Expedited Data Acknowledgement (EA)	DISCARD (c1)	DISCARD (c2)	NORMAL (c1)	NORMAL (c2)
Data (DT) and Data Acknowledgement (AK)	NORMAL (c1)	NORMAL (c2)	NORMAL (c3)	NORMAL (c4)

Legend for Table B-5/ATIS-1000112.4

NORMAL: The action taken by signaling point Y follows the normal procedures as defined in the appropriate sections of the procedure text.

DISCARD: Signaling point Y discards the received message and takes no subsequent action as a direct result of receiving that message.

ERROR: Signaling point Y discards the received message packet and indicates a reset by transmitting a RSR message with the appropriate cause indication (e.g., procedure error).

Annex C
(informative)

ANNEX C EXAMPLES OF SCCP ROUTING

C.1 Introduction

This Annex contains examples of addressing used in SCCP routing of connectionless messages. They are intended only to describe the use of global titles and the message return function, and should not be taken as a specification of how SCCP routing must be used. The point codes, subsystem numbers, and global title values are symbolic only.

C.2 Simple Global Title Translation

C.2.1 Successful Routing

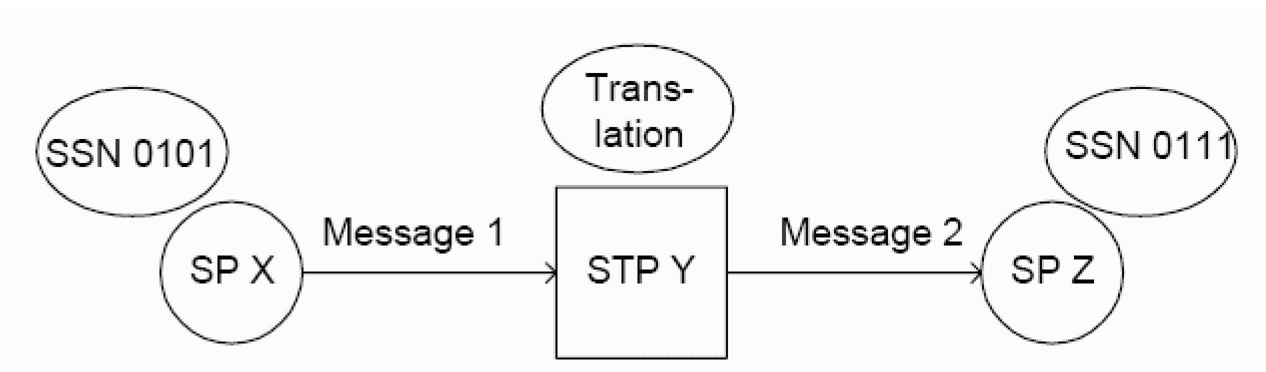


Figure C-1/ATIS-1000112.4 - Routing Model for Simple Translation

The initial message (Message 1) from SP X has address information coded as follows:

MTP information:

DPC = Y

OPC = X

SCCP information:

Cd Addr = GT + SSN, GT routing

GT = 201-758

SSN = 0000

Cg Addr = PC + SSN, SSN routing

PC = X

SSN = 0101

At STP Y, in this case GT translation results in GT 201-758 \(-> PC Z + SSN 0111. The subsequent message (Message 2) from STP Y to SP Z has the following address information:

MTP information:

DPC = Z

OPC = Y

SCCP information:

Cd Addr = GT + SSN, SSN routing

GT = 201-758

SSN = 0111

Cg Addr = PC + SSN, SSN routing

PC = X

SSN = 0101

C.2.2 Unsuccessful Routing

It is assumed here that message return on error has been requested by the sender, SP X. If message return was not requested, no *UDTS* message would be sent.

C.2.2.1 Scenario 1: Routing Problem at STP

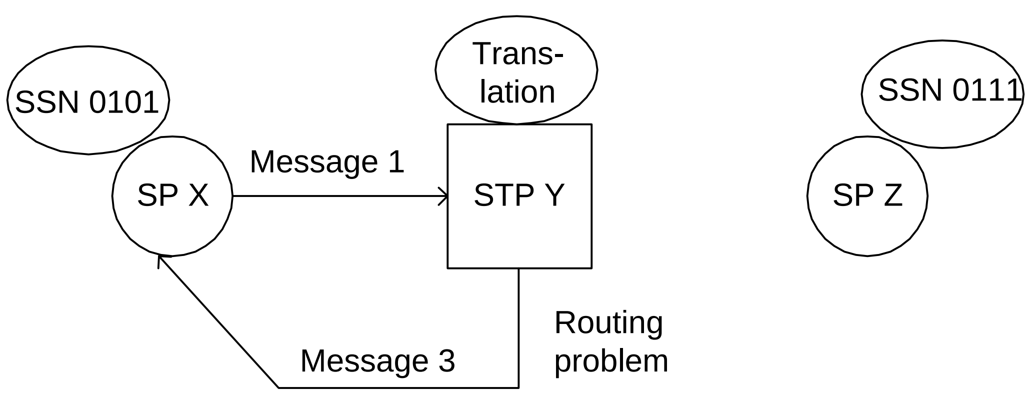


Figure C-2/ATIS-1000112.4 - Routing Problem at STP

In this case, a routing problem occurs at the STP, resulting in a *UDTS* message (Message 3) being returned to the sender with the following information:

MTP information:

DPC = X

OPC = Y

SCCP information:

Cd Addr = SSN, SSN routing
SSN = 0101
Cg Addr = GT + SSN, GT routing
GT = 201-758
SSN = 0000
Cause = No translation for this address, or no translation for this type of address, or network failure/ congestion, or subsystem failure/ congestion

NOTE - The Called Party Address may also contain point code X, if the *UDTS* is generated by modifying the pointer values to reverse the positions of the Calling and Called Party Address parameters. The point code would not be used by SCCP routing, and could be dropped if global title translation occurs in the reverse direction.

C.2.2.2 Scenario 2: Routing Problem at Terminating Node

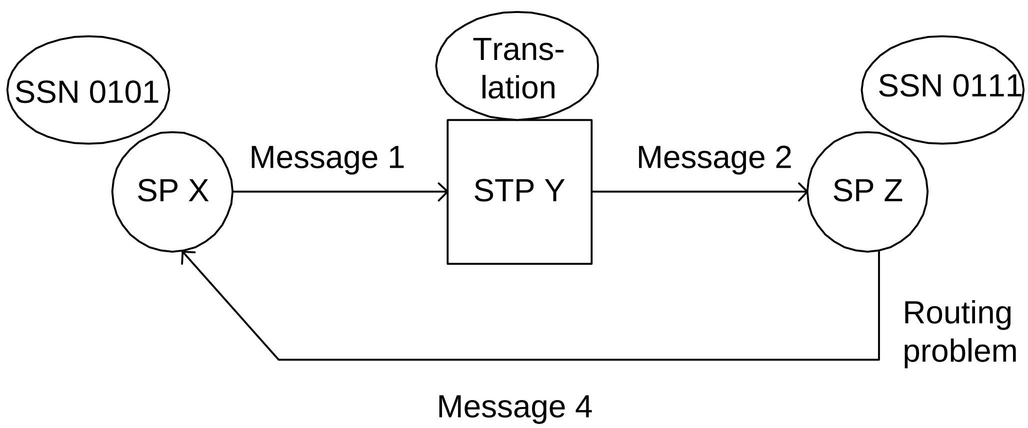


Figure C-3/ATIS-1000112.4 - Routing Problem at Terminating Node

In this case, a routing problem occurs at the terminating node, and if message return has been requested, the following *UDTS* message (Message 4) is returned to the sender:

MTP information:
DPC = X
OPC = Z
SCCP information:
Cd Addr = SSN, SSN routing
SSN = 0101
Cg Addr = GT + SSN, SSN routing
GT = 201-758

SSN = 0111

Cause = Subsystem failure, or

unequipped user

NOTE - If the pointer modification method is used, the Called Party Address would contain the point code X.

C.3 Routing with Distributed Translation Load

This clause provides an example of routing where different translator points perform global title translation for messages with different "classes" of global titles to be translated. This allows the total global title translation load to be distributed over a number of translator points, or STPs. One example of how global titles may be differentiated into "classes" would be to use the translation type.

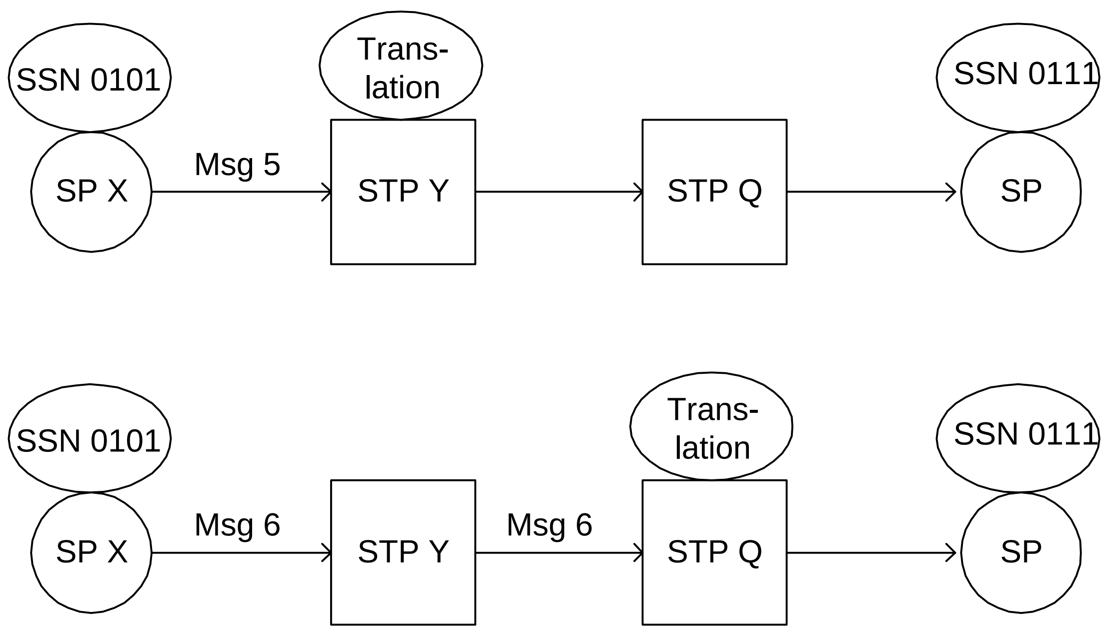


Figure C-4/ATIS-1000112.4 - Routing Model for Distributed Translation

The first message (Message 5) from SP X has the following address information:

MTP information:

DPC = Y

OPC = X

SCCP information:

Cd Addr=GT+SSN, GT routing

GT = 201-758, Type = A

SSN = 0000

Cg Addr=PC+SSN, SSN routing

PC = X

SSN = 0101

Messages with this type of global title address are directed toward STP Y for global title translation.

A second message (Message 6) from SP X carries a global title with a different translation type, as follows:

MTP information:

DPC = Q

OPC = X

SCCP information:

Cd Addr=GT+SSN, GT routing

GT = 201-758, Type = B

SSN = 0000

Cg Addr=PC+SSN, SSN routing

PC = X

SSN = 0101

In this case, messages with this type of global title address are passed through STP Y via MTP routing and directed toward STP Q for global title translation.

In either case, the translation of global titles at STP Y or STP Q follows the pattern for successful simple routing.

C.4 Routing with Multiple Translations

This clause provides models for routing where multiple translator points perform global title translations on a single message, from a user's perspective, during that message's transit.

C.4.1 Successful Routing

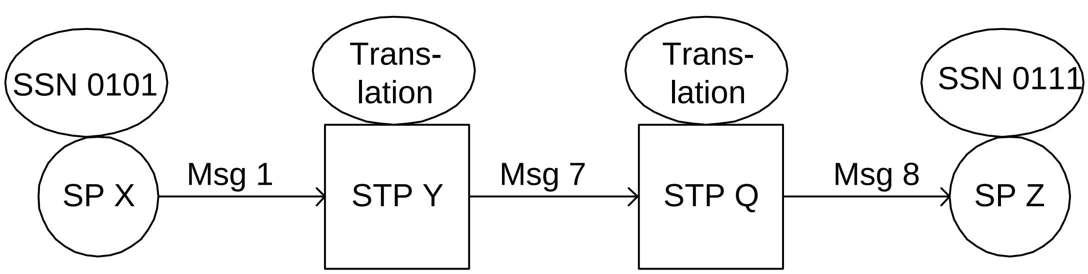


Figure C-5/ATIS-1000112.4 - Routing Model for Multiple Translations

Message 1 carries information as described in clause 2.1 of this Annex. In this case, GT translation at STP Y results in GT 201-758 -> PC Q and GT 212, and no SSN is determined. The subsequent message (Message 7) from STP Y takes the following address information:

MTP information:

DPC = Q

OPC = Y

SCCP information:

Cd Addr = GT + SSN, GT routing

GT = 212

SSN = 0000

Cg Addr = PC + SSN, SSN routing

PC = X

SSN = 0101

When this message is received at STP Q, a second translation takes place with a subsystem number and point code being identified, and Message 8 is forwarded to SP Z with the following address information:

MTP information:

DPC = Z

OPC = Q

SCCP information:

Cd Addr = GT + SSN, SSN routing

GT = 212

SSN = 0111

Cg Addr = PC + SSN, SSN routing

PC = X

SSN = 0101

C.4.2 Unsuccessful Routing

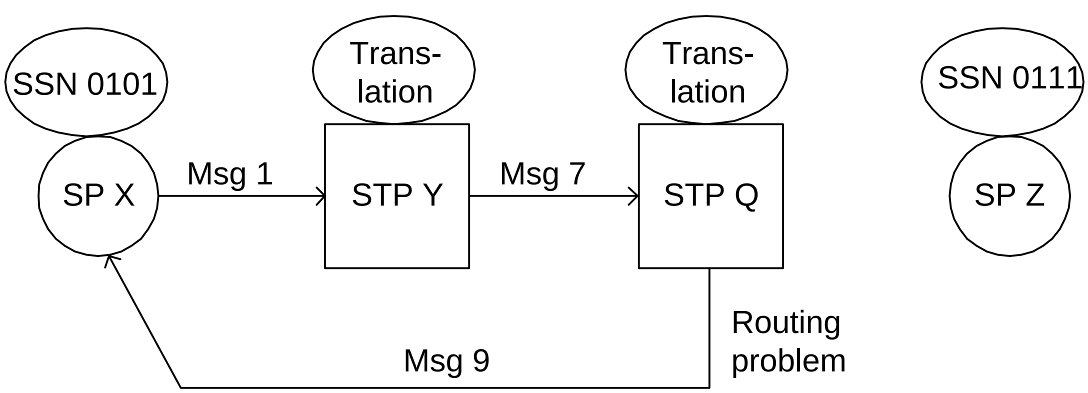


Figure C-6/ATIS-1000112.4 - Routing Problem at Second Translation Point

In this case, a routing problem has taken place at the second translation point. This problem results in the sending of a *UDTS* message (Message 9) back to the Calling Party with the following information:

MTP information:

DPC = X

OPC = Q

SCCP information:

Cd Addr = SSN, SSN routing

SSN = 0101

Cg Addr = GT + SSN, GT routing

GT = 212

SSN = 0000

Cause = No translation for this address, or no translation for this type of address, or network failure/ congestion, or subsystem failure/ congestion

In this case, the calling party cannot determine the original called party address value from the *UDTS* message, due to the intervening translation.

Annex D
(normative)

ANNEX D INTERMEDIATE SIGNALING NETWORK IDENTIFICATION PROCEDURES

This Annex contains the ISNI capability routing procedures. The SDLs for the protocol and procedures are in normative Annex E. Informative Annex F provides some examples of the ISNI protocol and procedures.

D.1 Protocol and Procedural Assumptions.

- No changes are needed to the interface between the SCCP and the MTP.
- The ISNI identification information is carried in the optional SCCP ISNI parameter in an *XUDT* message.
- ISNI information in the optional SCCP ISNI parameter serves the dual purpose of "identifying" networks as well as providing information that may help in the routing process. Thus, while the data is contained in one parameter, the functions of "identification" and "routing" are kept separate.
- The procedures at a SCCP Relay Node are consistent for all networks (i.e., origination, intermediate, and destination) and for all messages.
- The ISNI identification information, if present in the original message, may be used to route the *XUDTS* message through the same (series of) intermediate network(s), in reverse order.
- The identification function should not be performed on the *XUDTS* message. Therefore, the Mark for Identification Indicator in the *XUDTS* message should be ignored.

D.2 Procedures for ISNI Constrained Routing

D.2.1 Actions at the Origination SEP

When the SCCP at the Originating Node receives an N-UNITDATA request primitive from the Application containing the following ISNI information elements, the SCCP understands this as a request to format a *XUDT* message that includes the optional SCCP ISNI parameter with the following specified information:

- *Type of Routing indicator* - Which may take the values "constrained," "suggested," or "neither." (Suggested routing is for further study.);
- *Identification indicator* - Which may take the values "identify networks" or "do not identify networks;"
- *Type of ISNI indicator* - Which may be set to "Type 0 ISNI" or "Type 1 ISNI;"
- *Counter* - This value may be set to "zero" or "one" by the originating application as it provides an imaginary "pointer" which is used to locate routing and identification information. If the

originating application provides the identification for its own network, then the counter should be set to one.' Otherwise, the counter should be set to zero.

- *List of NIDs* - This is a list of Network IDs. The list may be empty when the message leaves the origination node if constrained routing is not requested. If the message route is to be constrained, then the originating application will include the NID(s) of the "specified" intermediate network(s) in the constrained routing information of the message.

All of the information above must be provided if the originating application requests ISNI constrained routing and/or ISNI identification. The detailed format of the ISNI parameter is shown in clause 6.2.2.

If return on error is set in the *XUDT* message and if ISNI routing is desired by the originator for the *XUDTS* message, then the Calling Party Address of the *XUDT* message must indicate routing on Global Title.

The message is then sent to a SCCP Relay Node for translation[22].

D.2.2 Actions at an ISNI-Capable SCCP Relay Node

D.2.2.1 Invocation of the ISNI Routing Function

When the SCCP *XUDT* message containing the ISNI parameter is received at an ISNI-capable SCCP Relay Node, the Routing Control Indicator of the ISNI parameter is examined to determine if the "Type of Routing indicator" is set to "constrained routing."

If the "Type of Routing Indicator" is set to "constrained routing" and if the Type 1 format is used, routing may be network-specific.

In the following, octet numbers in curly brackets ({}) refer to the type 0 format. Numbers in square brackets ([]) refer to the type 1 format.

Since each NID is fixed at 2 octets, the Counter in the Routing Control Indicator aids the SCCP Relay Node in locating an imaginary "pointer" at the beginning of the {2+2P}th [3+2P]th octet of the ISNI parameter, where P is the value of the Counter. The "pointer" is used to determine which NIDs should be used for routing and which NIDs should be considered identification information. The information below the "pointer" (i.e., the {2+2P}th [3+2P]th octet through the end of the parameter) is used for routing purposes while the information above the "pointer" (i.e., up to, but not including the {2+2P}th [3+2P]th octets) is identification information. Note that if P=0, there is no identification information in the message.

The following decision-making process is used by the SCCP Relay Node to perform ISNI routing:

a) The SCCP Relay Node checks the first NID after the "pointer," i.e., octets {2+2P}th [3+2P] and {3+2P} [4+2P], where P is the value in the Counter field. If this NID corresponds to

---

[22] The message is assumed to be addressed to an intermediate node (where translation occurs), since ISNI is invoked to assure that constrained routing, identification, or both will occur at one or more intermediate nodes in the message path. At this point, the next network that is required to be in the message path may be known only through its NID. Translation process yields either: 1) a full Point Code (PC) in that network; or 2) the PC of a node between the present node and that network. In the response message, the Global Title contains a Point Code and only one inter-network Translation Type value may be needed for response messages of this type regardless of their service type.

the network of this node, then the "pointer" is advanced by incrementing the value in the Counter field by one.

b) Step 1 is repeated. If this NID corresponds to the network of the node, then error handling procedures are initiated.

c) If the first NID after the pointer is not the same as the NID in the PC of this node, then this NID will be used as a "key" to "select" a DPC that will forward the message to another node along the path toward (or in) the specified network[23]. ISNI constrained routing results in the "selection" of a PC which is used as the DPC in the Routing Label of the transmitted message.

d) If there is no NID present after the "pointer," then routing will be performed based on the Called Party Address as described in ATIS-1000112.4.

If the "Type of Routing" indicator in the ISNI parameter is set to "Neither" (indicated by the IRI Routing Control Indicator), then ISNI routing will not be performed. Therefore, routing will be performed based on the Called Party Address as described in ATIS-1000112.4.

D.2.3 Actions at a Not-ISNI-Capable SCCP Relay Node

When a not-ISNI-capable node[24] receives an SCCP *XUDT* message with a "pointer to an optional part," it performs routing based on the SCCP Called Party Address as described in ATIS-1000112.4. There may be an "implicit relationship" between this network and some succeeding network in the message path. In this case, the GTT tables are configured to derive the DPC of a node in that particular succeeding network from the particular Global Title in the message.

The node must, at least, be able to recognize the *XUDT* message type and transmit another *XUDT* message with the ISNI optional parameter(s) unchanged. Otherwise, the *XUDT* message will be discarded.

D.2.4 Actions at the Destination SEP

The destination SEP does not perform any ISNI routing functions. When the destination node receives a *XUDT* message containing the ISNI parameter, the received ISNI parameter carried there is sent up to the SCCP User as parameters in the N-UNITDATA indication primitive.

D.2.5 Error Conditions

The following error conditions, which are specific to ISNI routing, would cause the error handling procedures to be invoked:

---

[23] The presence of the ISNI parameter does not by itself imply that the routing will be based on ISNI information. The data in this parameter serves the dual purpose of containing ISNI routing information as well as identification information if the application has requested "mark for identification."

[24] In what follows, not-ISNI-capable refers to the inability to parse and interpret the information in the ISNI parameter. It is assumed that the not-ISNI-capable SCCP Relay Node is capable of recognizing the *XUDT* message.

- The same network is specified two consecutive times in the list of NIDs.
- The message can not be routed toward the network(s) specified in the constrained routing information.
- An invalid ISNI routing request (e.g., suggested routing requested or network specific routing error) is received.

Other, non-ISNI specific, problems such as a hop counter violation, unauthorized message or message incompatibility would also invoke SCCP error handling procedures.

D.3 Procedures for Identification

D.3.1 Actions at the Origination SEP

See clause D.2.1.

D.3.2 Actions at an ISNI-Capable SCCP Relay Node

D.3.2.1 Invocation of Identification Function

Conceptually, this identification function follows the ISNI routing process. In the following, octet numbers in curly brackets ({}) refer to the type 0 format. Numbers in square brackets ([]) refer to the type 1 format.

The "mark for identification" indicator in the Routing Control Indicator is examined to determine if the identification function is requested. If identification is requested, indicated by the value of bit 1 in octet 1, the following decision-making process is followed to identify a network:

1. *If the value of the Counter is 0*, then any NIDs below the pointer is shifted down two octets and the resulting two empty octets below the pointer are filled with the NID of this node. Finally, the Counter is advanced to 1, indicating that the added NID is identification information. If the parameter length is greater than 14 before the NIDs are shifted, then error handling procedures are initiated.

   or:

1. *If the value of the Counter is non-zero*, the SCCP Relay Node examines the first NID above the "pointer" (octets {2P} [1+2P] and {1+2P} [2+2P], where P is the value in the Counter field). If this NID is the same as the NID in the PC of this node, then no further identification is required and the ISNI parameter is unchanged.
2. *In a small network*, if the two-octet NID does not match the Network Identifier and Cluster Identifier of this node, then any NIDs below the pointer are shifted down two octets and the resulting two empty octets below the pointer are filled with the NID of this node (i.e., the node "identifies itself"). *In a large network*, if the first octet of the NID is not the same as the first octet of the NID of this node's PC, then the node identifies itself. If the first octet of the NID is the same as the first octet of the NID of this node's PC but the second octet differs, the node may either: 1) make no change to the list; or 2) replace the second octet of the NID with the Cluster Identifier of this node.

If the "mark for identification" indicator in the ISNI parameter is set to "do not identify networks," then the ISNI parameter is transmitted without any change by the identification function.

D.3.3 Actions at a Not-ISNI-Capable SCCP Relay Node

The identification function cannot be performed at a not-ISNI-capable SCCP Relay node. The node must, at least, be able to recognize the *XUDT* message type and transmit another *XUDT* message with the ISNI optional parameter unchanged. Otherwise, the *XUDT* message will be discarded.

D.3.4 Actions at the Destination SEP

When the destination node receives an *XUDT* message containing the ISNI parameter, the received ISNI parameter carried there is sent up to the SCCP User as parameters in the N-UNITDATA indication primitive.

D.3.5 Error Conditions

The following error condition, which is specific to ISNI notification, would cause the error handling procedures to be invoked:

- There are no available fields in the ISNI parameter to add another NID to the list of NIDs when the identification function has been requested and another NID is to be added to the list.

D.4 Error Handling Procedures (Message Return)

When an *XUDT* message containing the ISNI parameter can not be transferred to its destination, the message return function will be initiated, if requested. The purpose of the message return function is to return an *XUDTS* message indicating that a message has encountered routing failure and cannot be delivered to its final destination. The procedure may be initiated, for example, as a result of insufficient translation information or the inaccessibility of a subsystem or Point Code.

1. If the undeliverable message is a *XUDT* message, and:
   a. The option field is set to "return message on error," then a *XUDTS* message is transferred to the Calling Party Address. (If the message is originated locally, an N-NOTICE indication primitive is invoked.)
   b. The option field is not set to "return message on error," then the message is discarded.
2. If the undeliverable message is a *XUDTS* message, then the message is discarded.

D.4.1 Procedures for Deriving the XUDTS Message

The node initiating the message return function should code the *XUDTS* message with the following information:

- The message type indicates an *XUDTS* message;

- ♦ The Return Cause field contains the reason for the message return. The possible cause values are:
  - o No translation for an address of such nature;
  - o No translation for this specific address;
  - o Subsystem congestion;
  - o Subsystem failure;
  - o Unequipped user;
  - o Network failure;
  - o Network congestion;
  - o Unqualified;
  - o Hop counter violation;
  - ∇ Unable to perform ISNI identification [11111110 (decimal 254)];
  - ∇ Redundant ISNI constrained routing information [11111101 (decimal 253)];
  - ∇ Cannot perform ISNI constrained routing. [11111100 (decimal 252)];
  - o Message incompatibility [11111011 (decimal 251)];
  - o Unauthorized request [11111010 (decimal 250)];
  - ∇ Invalid ISNI routing request [11111001 (decimal 249)];
  - ∇ - ISNI specific return causes;
- ♦ Pointers to the following parameters should be provided:
  - o Called Party Address;
  - o Calling Party Address;
  - o Data;
  - o Optional Parameter(s).
- ♦ The SCCP Called Party Address is based on the Calling Party Address in the *XUDT* message;
- ♦ The SCCP Calling Party Address is based on the Called Party Address in the *XUDT* message;
- ♦ The Data field in the *XUDTS* message should be identical to that contained in the *XUDT* message;
- ♦ The *XUDTS* message should contain the ISNI parameter as possibly modified in this node by the ISNI constrained routing information and/or ISNI identification functions. The value of the Mark for Identification bit is ignored since the identification function is not performed on a *XUDTS* message;
- ♦ The *XUDTS* message should be sent with the hop counter value reset to 15.

D.4.2 Procedures at SCCP Relay Nodes

D.4.2.1 Actions at an ISNI-Capable SCCP Relay Node

D.4.2.1.1 Invocation of the ISNI Routing Function

When the *XUDTS* message containing the ISNI parameter is received at an ISNI-capable SCCP Relay Node, the Routing Control Indicator is examined to determine the setting of the Type of Routing indicator. If the indicator is set to "Neither," then ISNI routing will not be performed. In this case, routing is performed based on the Called Party Address as described in ATIS-1000112.4.

If the indicator is set to "Constrained," then ISNI routing will be performed. Since the length of the NID field is fixed (i.e., at 2 octets), the Counter in the Routing Control Indicator aids the SCCP Relay Node in locating an imaginary pointer at the beginning of the {2+2P}th [3+2P]th octet of the ISNI parameter, where P is the value of the Counter. The pointer is used to determine which NIDs should be used for routing. The information in the {second} [third] through {1+2P}th [2+2P]th octets is used for routing. Note that if P=0, there is no routing information in the message. In this case, routing is performed based on the Called Party Address as described in ATIS-1000112.4.

The following decision-making process is used by the SCCP Relay Node to perform ISNI routing:

1. The SCCP Relay Node checks the NID in octets {2P} and {1+2P} [1+2P] and [2+2P], where P is the value of the Counter field. If this NID is the same as the NID in the PC of this node, then the pointer is changed by decrementing the value in the Counter field by one;
2. If the value in the Counter field is now zero, routing is performed based on the Called Party Address as described in ATIS-1000112.4;
3. If the Counter field is non-zero and the NID in octets {2P} and {1+2P} [1+2P] and [2+2P] is not the same as the NID in the PC of this node, then this NID will be used as a "key" to select a DPC that will forward the message along the path toward (or in) the specified network.

The translation results in the selection of a PC which is used as the DPC in the Routing Label of the transmitted message.

D.4.2.1.2 Invocation of the ISNI Identification Function

A SCCP relay node should not perform the ISNI Identification function on a *XUDTS* message. The Mark for Identification bit in the ISNI parameter is ignored.

D.4.2. Actions at a Not-ISNI-Capable SCCP Relay Node

When a not-ISNI-capable node receives a *XUDTS* message with a "pointer to an optional part," it performs routing based on the SCCP Called Party Address as described in ATIS-1000112.4. There may be an "implicit relationship" between this network and some succeeding network in the message path. In this case, the GTT tables are configured to derive the DPC of a node in that particular succeeding network from the particular Global Title in the message. If the *XUDTS* message can not be routed, then it should be discarded.

The not-ISNI-capable node must, at least, be able to recognize the *XUDTS* message type and transmit another *XUDTS* message with the ISNI optional parameter unchanged. Otherwise, the *XUDTS* message will be discarded.

D.4.3 Actions at the Destination Node

When a *XUDTS* message is received at the destination node, a N-NOTICE indication primitive is invoked.

Annex E
(normative)

ANNEX E INTERMEDIATE SIGNALING NETWORK IDENTIFICATION SDL

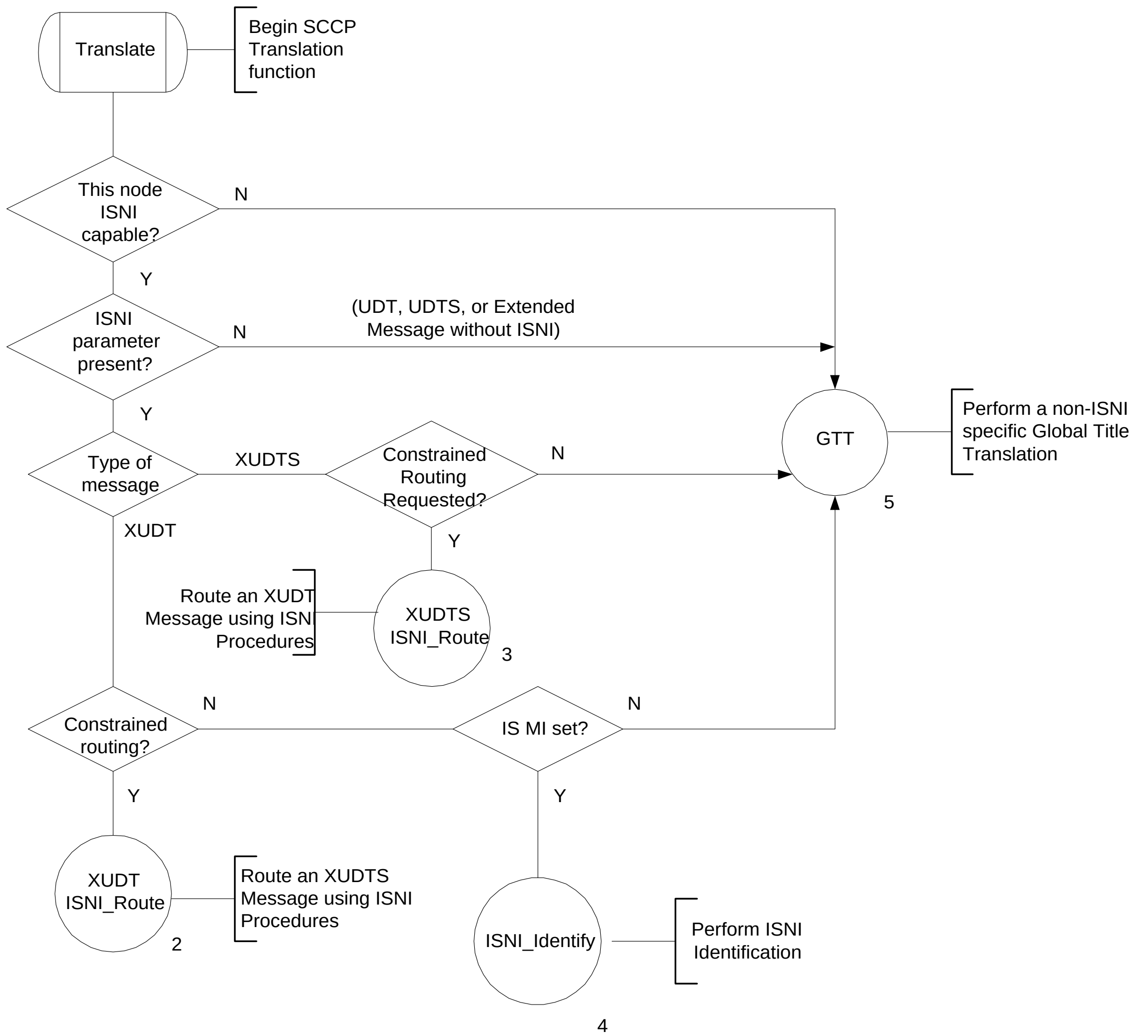


Figure E-1/ATIS-1000112.4 - ISNI SDL (sheet 1 of 5)

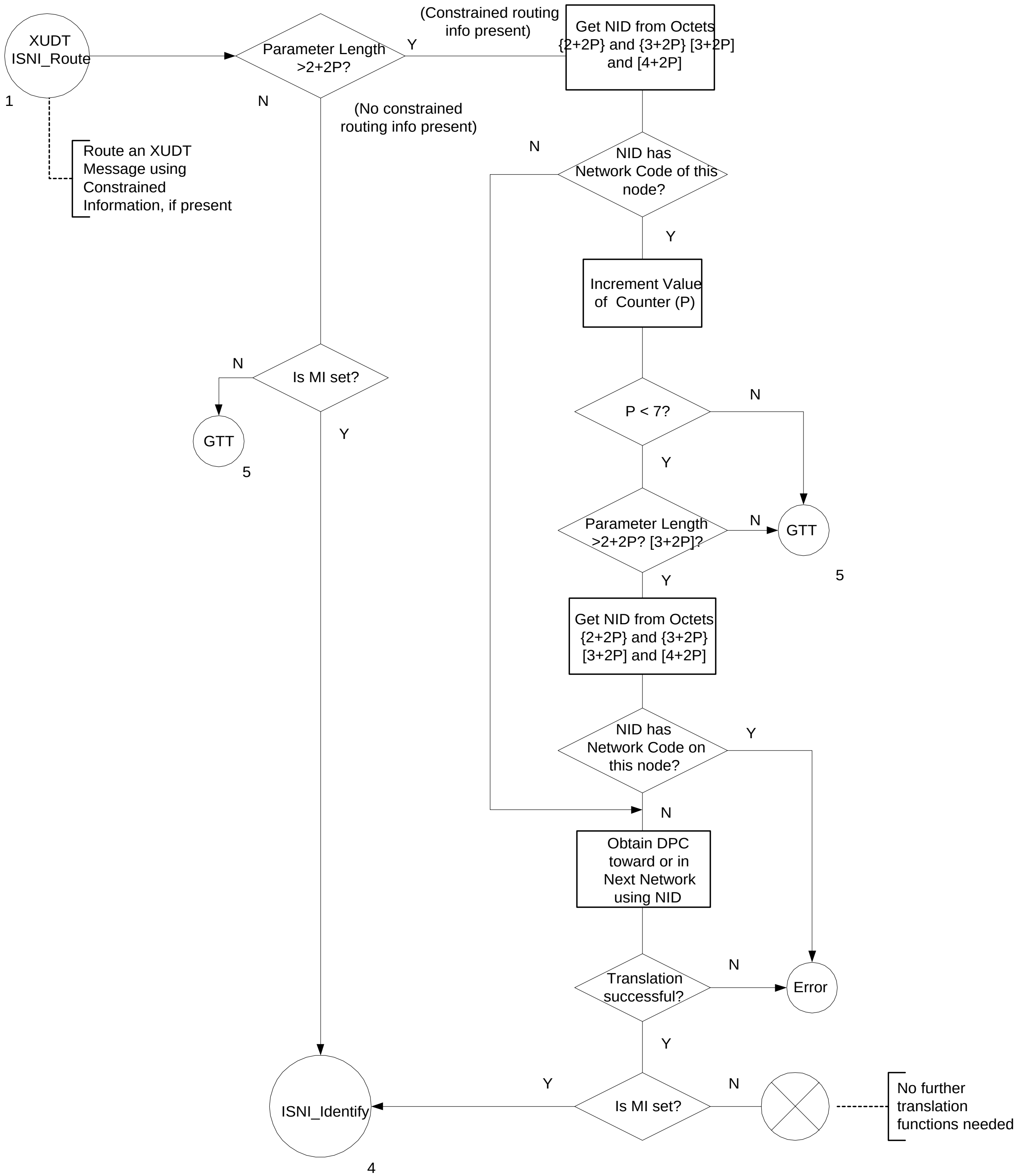


Figure E-1/ATIS-1000112.4 - ISNI SDL (sheet 2 of 5)

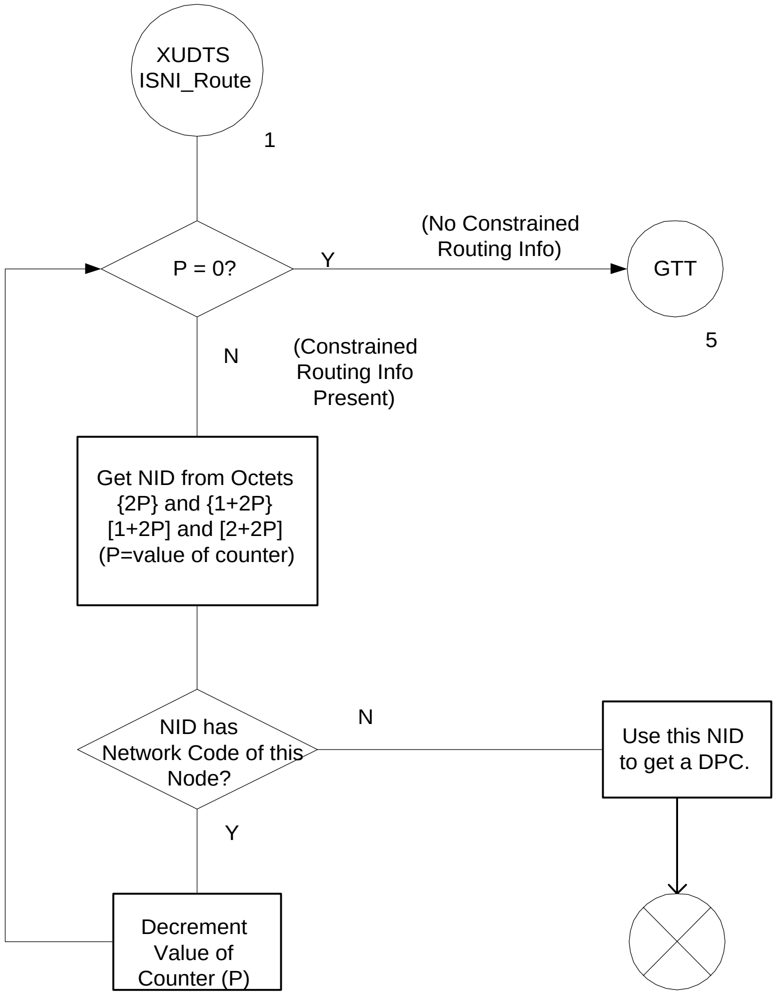


Figure E-1/ATIS-1000112.4 - ISNI SDL (sheet 3 of 5)

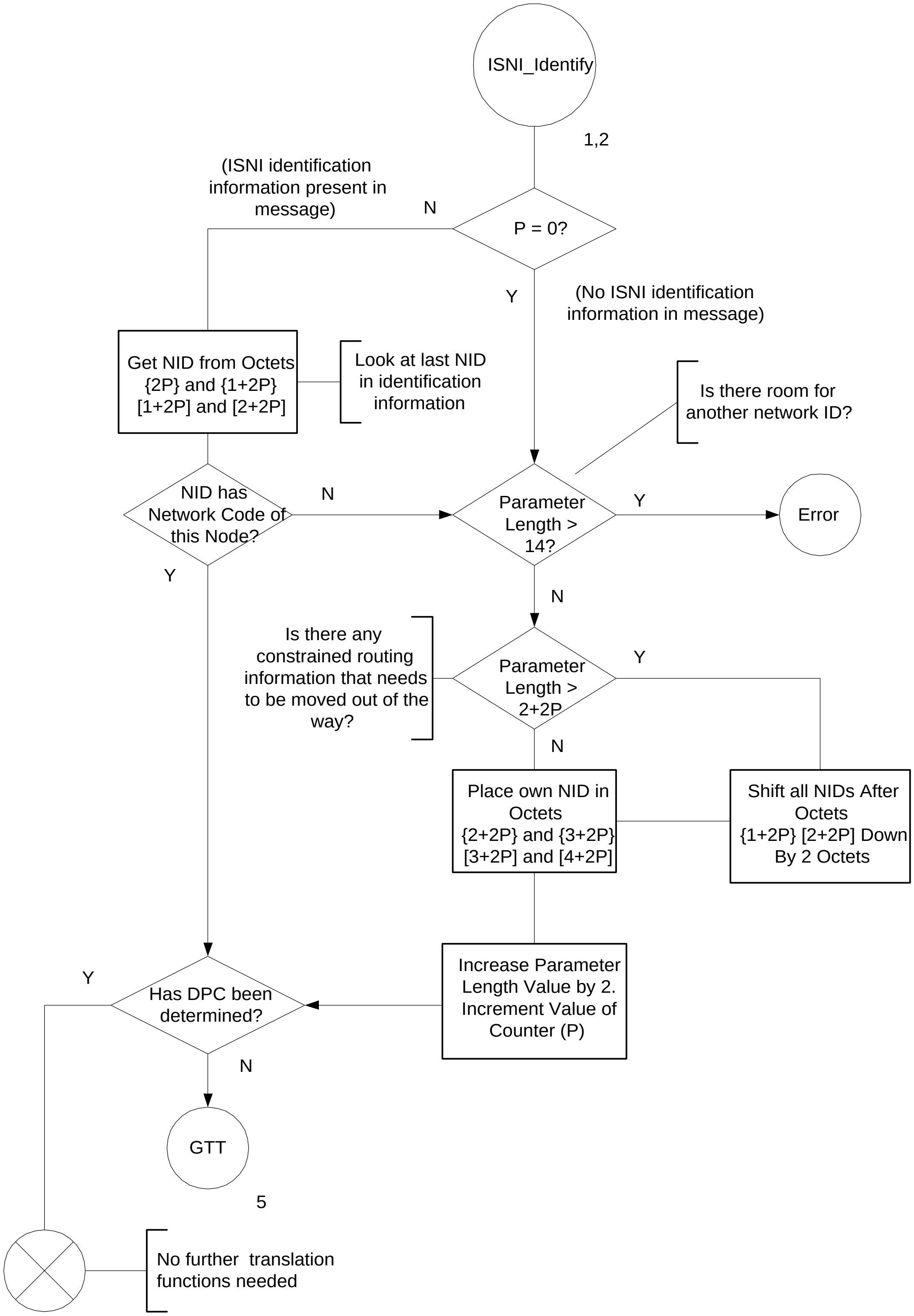


Figure E-1/ATIS-1000112.4 - ISNI SDL (sheet 4 of 5)

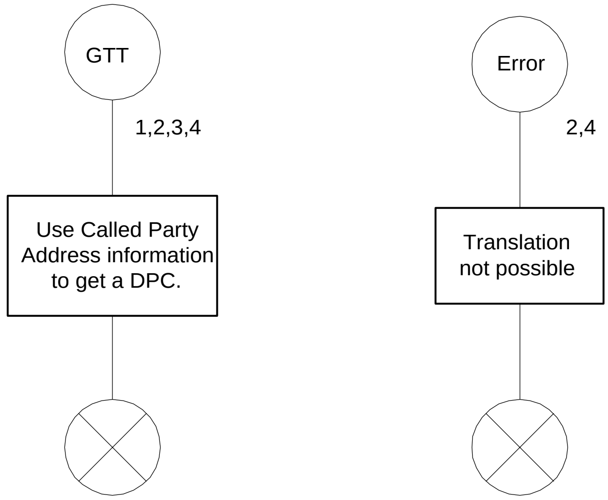


Figure E-1/ATIS-1000112.4 - ISNI SDL (sheet 5 of 5)

Annex F
(informative)

ANNEX F EXAMPLES OF ISNI MESSAGE CONTENT

Figure F-1/ATIS-1000112.4 shows a message path from origination network A, through a branch point STP (2) in the origination network, passing through two intermediate networks (B and C) to reach destination network D. The following Tables show the pertinent message content as the messages traverse the networks and are modified by the translating STPs.

In Figure F-1/ATIS-1000112.4, the digits under each symbol denote the SS7 Point Code of their respective nodes. The letters denote the ISNI NIDs corresponding to their respective networks.

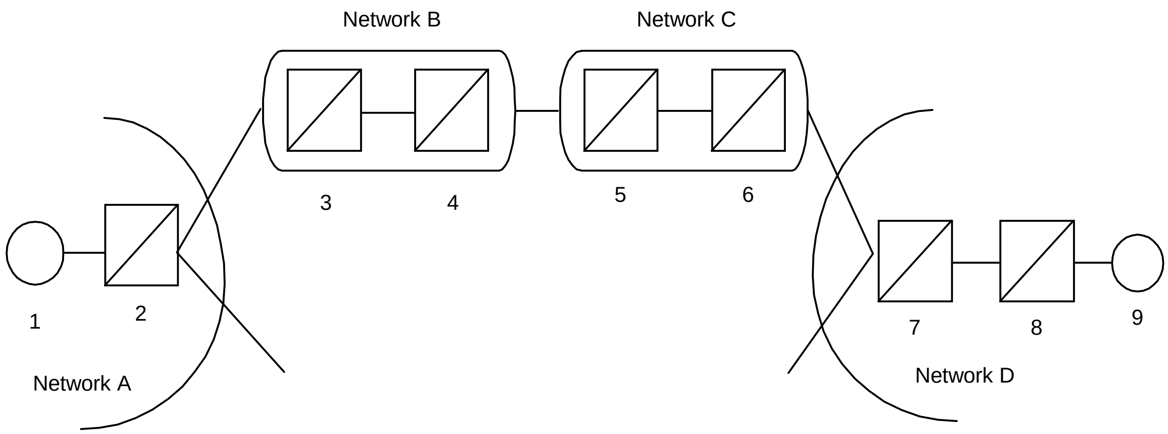


Figure F-1 ATIS-1000112.4 - Reference ISNI Message Path

In the tables, GT(x) denotes a Global Title that will eventually be translated to the Point Code of node x and the appropriate SSN at that node (denoted SSN = x). For ease of reading, the Point Code and SSN at a node are assigned the same digit. In addition, the following abbreviations are used:

CdPA -	SCCP Called Party Address
CgPA -	SCCP Calling Party Address
Counter -	Counter in the ISNI Parameter (range 0 to 7)
List -	The List of NIDs in the ISNI Parameter

F.1 Example of Constrained Routing Only

In this example, the originating application constrains the message to traverse networks B and C to reach network D. Including the NID of network D in the constrained routing list is not necessary to deliver the message to node 9.

Table F-1/ATIS-1000112.4 - Constrained Routing Only

Message leaving node #	MTP		SCCP					
	OPC	DPC	Cd PA	Cg PA	Counter	List		
1	1	2	GT(9)	PC=1, SSN=1	0	B	C	D
2	2	3	GT(9)	PC=1, SSN=1	0	B	C	D
3	3	5	GT(9)	PC=1, SSN=1	1	B	C	D
4	3	5	GT(9)	PC=1, SSN=1	1	B	C	D
5	5	7	GT(9)	PC=1, SSN=1	2	B	C	D
6	5	7	GT(9)	PC=1, SSN=1	2	B	C	D
7	7	9	PC=9, SSN=9	PC=1, SSN=1	3	B	C	D
8	7	9	PC=9, SSN=9	PC=1, SSN=1	3	B	C	D

F.2 Example of Identification Only

In this example, the originating application does not constrain the message route, but the message traverses networks B and C to reach network D. The originating application requests identification and an ISNI-capable STP in each network inserts its NID into the list.

Table F-2/ATIS-1000112.4 - Identification Only

Message leaving node #	MTP		SCCP					
	OPC	DPC	Cd PA	Cg PA	Counter	List		
1	1	3	GT(9)	PC=1, SSN=1	0			
2	1	3	GT(9)	PC=1, SSN=1	0			
3	3	5	GT(9)	PC=1, SSN=1	1	B		
4	3	5	GT(9)	PC=1, SSN=1	1	B		
5	5	7	GT(9)	PC=1, SSN=1	2	B	C	
6	5	7	GT(9)	PC=1, SSN=1	2	B	C	
7	7	9	PC=9, SSN=9	PC=1, SSN=1	3	B	C	D
8	7	9	PC=9, SSN=9	PC=1, SSN=1	3	B	C	D

F.3 Unconstrained Query with Identification, Constrained Reply

In this example, the querying application does not include any anticipation notification information in the query. Instead, the query is marked for identification. Table F-3/ATIS-1000112.4 shows the message content as the query message leaves each node.

Table F-3/ATIS-1000112.4 -Query With Identification Only

Message leaving node #	MTP		SCCP					
	OPC	DPC	Cd PA	Cg PA	Counter	List		
1	1	3	GT(9)	PC=1, SSN=1	0			
2	1	3	GT(9)	PC=1, SSN=1	0			
3	3	5	GT(9)	PC=1, SSN=1	1	B		
4	3	5	GT(9)	PC=1, SSN=1	1	B		
5	5	7	GT(9)	PC=1, SSN=1	2	B	C	
6	5	7	GT(9)	PC=1, SSN=1	2	B	C	
7	7	9	PC=9, SSN=9	PC=1, SSN=1	3	B	C	D
8	7	9	PC=9, SSN=9	PC=1, SSN=1	3	B	C	D

The queried application receives the identification notification information. This information notifies the queried application that networks B, C, and D were transited. The queried application could recognize that it is part of network D and exclude this code from the constrained routing information in the reply message. This example illustrates that there is no harm in including this network code. If the querying application requires notification information, this may be carried as anticipation information.

Table F-4/ATIS-1000112.4 shows the message content as the reply message leaves each node.

Table F-4/ATIS-1000112.4 - Reply With Constrained Routing Only

Message leaving node #	MTP		SCCP					
	OPC	DPC	Cd PA	Cg PA	Counter	List		
9	9	7	GT(1)	PC=9, SSN=9	0	D	C	B
8	9	7	GT(1)	PC=9, SSN=9	0	D	C	B
7	7	6	GT(1)	PC=9, SSN=9	1	D	C	B
6	6	4	GT(1)	PC=9, SSN=9	2	D	C	B
5	6	4	GT(1)	PC=9, SSN=9	2	D	C	B
4	4	2	GT(1)	PC=9, SSN=9	3	D	C	B
3	4	2	GT(1)	PC=9, SSN=9	3	D	C	B
2	2	1	PC=1, SSN=1	PC=9, SSN=9	3	D	C	B

Note that if identification is requested on the reply message, STP 2 would insert its network code in the message. If network D is not included in the message as sent from node 9 and identification is requested, STP 7 would insert its network code in the message.

F.4 Constrained Query with Identification, Constrained Reply

In this example, the querying application constrains the query to transit networks B and C marks the query for identification. Figure F-1/ATIS-1000112.4 shows a message path from origination network A, through a branch point STP (2) in the origination network, passing through two intermediate networks (B and C) to reach destination network D. Table F-5/ATIS-1000112.4 shows the message content as the query message leaves each node.

Table F-5/ATIS-1000112.4 - Query With Constrained Routing and Identification

Message leaving node #	MTP		SCCP						
	OPC	DPC	Cd PA	Cg PA	Counter	List			
1	1	2	GT(9)	PC=1, SSN=1	0	B	C		
2	2	3	GT(9)	PC=1, SSN=1	1	A	B	C	
3	3	5	GT(9)	PC=1, SSN=1	2	A	B	C	
4	3	5	GT(9)	PC=1, SSN=1	2	A	B	C	
5	5	7	GT(9)	PC=1, SSN=1	3	A	B	C	
6	5	7	GT(9)	PC=1, SSN=1	3	A	B	C	
7	7	9	PC=9, SSN=9	PC=1, SSN=1	4	A	B	C	D
8	7	9	PC=9, SSN=9	PC=1, SSN=1	4	A	B	C	D

Note that STP 2 identifies itself, as any other STP in the message path does. To do this, it right-shifts the other network codes in the parameter to make room for its code. Similarly, STP 7 identifies itself.

The queried application receives the identification notification information. This information notifies the queried application that networks A, B, C, and D were transited. The queried application recognizes that it is part of network D and may optionally exclude this code from the constrained routing information in the reply message, as shown in this example. Similarly, if the queried application recognizes that network A is the destination network for the reply message, it may exclude the code of destination network A. Table F-6/ATIS-1000112.4 shows the message content as the reply message leaves each node.

Table F-6/ATIS-1000112.4 - Reply With Constrained Routing Only

Message leaving	MTP		SCCP					
node #	OPC	DPC	Cd PA	Cg PA	Counter	List		
9	9	7	GT(1)	PC=9, SSN=9	0	C	B	
8	9	7	GT(1)	PC=9, SSN=9	0	C	B	
7	7	6	GT(1)	PC=9, SSN=9	0	C	B	
6	6	4	GT(1)	PC=9, SSN=9	1	C	B	
5	6	4	GT(1)	PC=9, SSN=9	1	C	B	
4	4	2	GT(1)	PC=9, SSN=9	2	C	B	
3	4	2	GT(1)	PC=9, SSN=9	2	C	B	
2	2	1	PC=1, SSN=1	PC=9, SSN=9	2	C	B	

Note that if identification is requested on the reply message, STP 2 would insert its network code in the message. If network D is not included in the message as sent from node 9 and identification is requested, STP 7 would insert its network code in the message.

F.5 An Example of an Undeliverable Message, XUDTS *Message Return*

Consider a message path as in Figure F-1/ATIS-1000112.4 with a message starting in Network A, transiting Networks B and C, and encountering a routing problem at node 7 in Network D. Table F-7/ATIS-1000112.4 shows the MTP and SCCP routing information as the query leaves each node en route to node 9. A *XUDTS* message returned from node 7 (to node 1) is shown in Table F-8/ATIS-1000112.4.

Table F-7/ATIS-1000112.4 - Query Encountering Problems with Constrained Routing and Identification

Message leaving	MTP		SCCP					
node #	OPC	DPC	C′ dPA	C′ gPA	Counter	List		
1	1	2	GT(9)	GT(PC=1)	0	B	C	
2	2	3	GT(9)	GT(PC=1)	1	A	B	C
3	3	5	GT(9)	GT(PC=1)	2	A	B	C
4	3	5	GT(9)	GT(PC=1)	2	A	B	C
5	5	7	GT(9)	GT(PC=1)	3	A	B	C
6	5	7	GT(9)	GT(PC=1)	3	A	B	C
7								

Table F-8/ATIS-1000112.4 - XUDTS Message Returned with Constrained Routing

Message leaving node #	MTP		SCCP					
	OPC	DPC	C′ dPA	C′ gPA	Counter	List		
7	7	6	GT(PC=1)	GT(9)	3	A	B	C
6	6	4	GT(PC=1)	GT(9)	2	A	B	C
5	6	4	GT(PC=1)	GT(9)	2	A	B	C
4	4	2	GT(PC=1)	GT(9)	1	A	B	C
3	4	2	GT(PC=1)	GT(9)	1	A	B	C
2	2	1	PC=1, SNN=1	GT(9)	0	A	B	C

Annex G
(normative)

ANNEX G INTERMEDIATE NETWORK SIGNALING (INS) PROCEDURES

G.1 Protocol and Procedural Assumptions

- No changes are needed to the interface between the SCCP and the MTP.
- The information that is used to select the desired intermediate network is carried in an optional SCCP parameter in an *XUDT* message.
- The originating node will select only one intermediate CCS network (ICN).[25]
- The SCCP Relay Node procedures described here apply in any network (i.e., origination, intermediate, and destination) that is capable of supporting the processing described herein. This capability interworks appropriately in situations where the INS functionality is only supported in the origination network, and subsequent networks support, at a minimum, GTT capability.
- Any specification information used in the forward direction, if present, will be used to route the *XUDTS* message through the same intermediate network in the reverse direction.
- Any INS-capable node will be aware of the INS capability of an adjacent node.

G.2 Formats of the Optional SCCP INS Parameter

The INS parameter format is given in the following figure. Depending on the value of the Information Type, the fourth and fifth octets will be encoded in SS7 format as a combination of “network codes” plus “cluster codes,” or as a two-octet network-specific identifier.

If encoded in SS7 format, the Network ID will contain the following:

- For large networks, the first octet is the NID in the SS7 Point Code (the second octet may be coded with a cluster value or with all zeros).
- For small networks, two octets are required to identify the network.

[25] The capability for the originating node to identify more than one selected network, specifically for constrained routing, is beyond the scope of this document.

H	G	F	E	D	C	B	A
Name of Parameter (INS)							
Length Of Parameter							
Counter		Res		Type of Routing		Info Type	
Network Identifier 1 (2 octets)							
Network Identifier 2 (2 (octets)							

Figure G-1/ATIS-1000112.4 - INS Parameter

- *Counter* - The counter provides an imaginary "pointer" which is used to locate routing information. The possible counter values for INS are 0, 1, and 2. If the counter is 0, then none of the routing information in the INS parameter has been used (i.e., all of the routing information is yet to be used). If the counter is 1, then the first piece of routing information (i.e., Network ID 1) should not be used any further in routing the message. If the counter is 2, then neither the first nor the second Network IDs should not be used in subsequent routing of the message. The counter is advanced when the referenced routing information is not to be used in subsequent routing of the message.

- *Reserved* - One possible use of the "reserved" field in the parameter would be to indicate that this parameter could be "dropped" (i.e., during Message Change from *XUDT* to *UDT*). The use of the "reserved" field as an indicator for message conversion is for further study.

- *Type of Routing* - This field indicates the type of INS routing that should be applied to the message.

  00 Neither Constrained Nor Suggested INS Routing
  01 Constrained INS Routing
  10 Suggested INS Routing
  11 Reserved

- *Information Type Indicator* - This field identifies the coding format used for the information in the first Network Identifier field. An information type of "SS7 Format" indicates that the network identifier will be encoded in SS7 format as a combination of "network codes" plus "cluster codes" as defined in ATIS-1000111.4.

  00 SS7 Format
  01 reserved
  10 Network-Specific 1
  11 Network-Specific 2

- *Network Identifiers* - The information in the Network Identifier fields specifies the routing information. If the Information Type indicates that the network identifier is encoded in SS7 format, the first Network Identifier will consist of a network code and cluster code. Other values of the first Network Identifier field will be encoded based on future definition of the network-specific information types. The second Network Identifier is encoded in SS7 format.

G.3 Procedures for Routing Using the INS Capability

G.3.1 Actions at the Origination SEP

When the SCCP at the Originating Node receives an N-UNITDATA request primitive from the Application containing the following information elements, the SCCP understands this as a request to format an *XUDT* message that includes the optional SCCP INS parameter with the specified information.

- *Counter* - "Pointer" which is used to indicate which routing information has already been used (i.e., information that is not to be used for subsequent routing).
- *Type of Routing indicator* - Which may take the values "constrained," "suggested," or "neither."
- *Information type* - Which indicates whether the first Network ID is encoded in "SS7 Format" or a network-specific format.
- *Selected Intermediate Network* - This is the Network ID associated with the selected intermediate signaling network.

The format of the optional SCCP INS parameter is shown in clause G.2.

If return on error is set in the *XUDT* message and if symmetric routing is desired by the *XUDT* originator for the *XUDTS* message, then the Calling Party Address of the *XUDT* message must indicate routing on Global Title.

The message is then sent to an SCCP Relay Node.

G.3.2 Actions at the INS Capable SCCP Relay Node

G.3.2.1 Invocation of the INS Function

When the *XUDT* message containing the INS parameter is received at an INS-capable SCCP Relay Node, the INS parameter is examined to determine if the "Type of Routing indicator" is set to "constrained routing," "suggested routing," or “neither constrained nor suggested routing.” Depending on the value, one of the following sets of procedures should be followed.

1. If the "Type of Routing Indicator" is set to "*constrained routing*”:

   (a) The SCCP Relay node checks to see if there are any unused NIDs.

   - If not, a DPC is derived based on the TT and GTA in the SCCP Called Party Address.
   - If so, the SCCP Relay Node determines whether the "next" NID (the “counter value + 1” NID, i.e., the first NID if counter = 0, or the second NID, if present and counter = 1) identifies the network in which the current SCCP Relay node resides.

   (b) If the NID identifies the network in which the current SCCP Relay node resides, the counter is incremented and step a is repeated. If the NID identifies a different network, a PC is derived based on the NID.

(c) If the Information Type in the received INS parameter is encoded with a value other than "SS7 Format," an SS7 Format NID is substituted for the network specific information, and the value of the Information Type indicator is changed to "SS7 Format;" otherwise, the NID and the Information Type are left unchanged.

(d) If the derived PC is not in the network identified by the NID and is not INS-capable, SCCP routing failure procedures apply. However, if it is INS-capable (but not in the network identified by the NID), the routing label is populated with the derived PC and the *XUDT* message is routed, if the DPC is available.

(e) If the derived PC is in the network identified by the NID, the counter is incremented.

- ♦ If the derived PC is not INS-capable, and there are unused NIDs, SCCP routing failure procedures apply. However, if there are no unused NIDs and the next node is XUDT-capable, the routing label is populated with the derived PC and the XUDT message is routed, if the DPC is available. If there are no unused NIDs and the next node is not XUDT-capable, the message is reformatted as a UDT message, the routing label is populated with the derived PC and the UDT message is routed, if the DPC is available.
- ♦ If the derived PC is INS-capable, the routing label is populated with the derived PC and the XUDT message is routed, if the DPC is available.

2. If the "Type of Routing Indicator" is set to "*suggested routing*":

(a) The SCCP Relay node performs a GTT using the received TT and GTA information in the Called Party Address.

- ♦ If the resulting PC is associated with an end node, and routing to that PC does not require the use of an ICN, the DPC of the routing label is populated with the PC and the *XUDT* message is routed. The INS parameter is unchanged.
- ♦ If the resulting PC is associated with another SCCP Relay Node and routing to that PC does not require the use of an ICN (i.e., first SCCP Relay Node performs a non-final GTT), the *XUDT* message is routed to the next SCCP Relay Node for further GTT. The INS parameter is unchanged.
- ♦ If the resulting PC is associated with a node that must be routed to via an ICN, the SCCP Relay Node continues processing as described in b) below.

(b) An SCCP Relay Node may include a second NID field (in SS7 format) in the INS parameter identifying the network associated with the PC that was determined as a result of the GTT/NPGTT processing that was performed on the Called Party Address information. If a second NID is added to the INS parameter, INS processing should change the value of the "Type of Routing" indicator to "constrained." If a second NID field is not added to the INS parameter, INS processing may leave the "Type of Routing" indicator as "suggested." Depending on the processing performed by the current SCCP Relay Node and the functionality available at the next SCCP Relay Node, the current SCCP Relay Node may or may not decide to add a second NID to the INS parameter. If a second NID is not added to the INS parameter, the SCCP Relay node may or may not change the value of the "Type of Routing" indicator to "constrained."[26]

If the "Type of Routing" indicator is changed to constrained, the procedures described in Item 1 are invoked. If the "Type of Routing" indicator remains "suggested," INS processing continues with step c) below.

(c) If there are no unused NIDs, and:

- ♦ The next node is XUDT-capable, the DPC of the routing label is populated with the derived PC (from the GTT) and the XUDT message is routed with the INS parameter unchanged.
- ♦ The next node is not XUDT-capable, the message is reformatted as a UDT message and routed based on the DPC that resulted from the GTT (or NPGTT processing).

(d) If there are unused NIDs, and:

- ♦ The NID identifies the same network as the one in which the SCCP Relay Node resides, the counter is incremented and step (c) is repeated.
- ♦ The NID identifies a different network, the SCCP Relay Node derives a PC based on the NID and proceeds as follows:
  - o If the counter = 1, the procedures for constrained routing are followed, beginning at step b).
  - o If the counter = 0, the SCCP Relay node identifies the "next" NID (i.e., the first NID) in the INS parameter. If the NID is not in SS7 format, the SCCP Relay node associates an SS7-formatted NID (i.e., "network and cluster") with the network-specific routing information, and proceeds as described below using the SS7-formatted NID value.

(e) If the derived PC is in the network identified by the NID, the counter is incremented and the procedures described below in (g) are followed.

(f) If the derived PC is not in the network identified by the NID, and

- ♦ The derived DPC is not in the same network as the current SCCP relay node, the procedures described below in (g) are followed.
- ♦ The derived DPC is in the same network as the current SCCP relay node (but not in the network identified by the NID), the routing indicator within the INS parameter of the outgoing XUDT must be changed to constrained.[27] If the derived PC is INS capable, the DPC of the routing label is populated with the derived PC and the XUDT message is routed, if the DPC is available. If the derived PC is not INS-capable, the message fails.

---

[26] As described below, the only time it is critical that the value of the "Type of Routing" indicator be changed to "constrained" is when the derived PC identifies the preceding SCCP Relay Node. Otherwise, it is the decision of the network provider whether the "Type of Routing" indicator will be left as "suggested" or changed to "constrained" when a second NID is not added to the INS parameter.

[27] This will prevent looping between the node associated with the derived DPC and the current SCCP Relay node.

(g) If the derived PC is neither INS-capable nor *XUDT*-capable, the SCCP Relay Node reformats the message as a *UDT* message, populates the DPC of the routing label with the derived PC and routes the *UDT* message, if the DPC is available.

If the derived PC is INS-capable or *XUDT*-capable, the DPC of the routing label is populated with the derived PC and the *XUDT* message is routed, if the DPC is available.

3. If the "Type of Routing Indicator" is set to "neither constrained nor suggested routing" then INS routing will not be performed. Routing will be performed based on the Called Party Address as described in ATIS-1000112.4.

G.3.3 Actions at a Non-INS-Capable SCCP Relay Node

If a non-INS-capable node[28] is capable of recognizing an *XUDT* message and it receives an *XUDT* message with a "pointer to an optional part" and an INS parameter, it should perform routing based on the SCCP Called Party Address as described in ATIS-1000112.4. There may be an "implicit relationship" between this network and some succeeding network in the message path. In this case, the GTT tables are configured to derive the DPC of a node in that particular succeeding network from the particular Global Title in the message. The node should forward the *XUDT* message with the INS optional parameter unchanged.

If a non-INS-capable node is also not *XUDT* capable (i.e., is unable to recognize an *XUDT* message) and it receives an *XUDT* message that contains an INS parameter, it will discard the received *XUDT* message.

G.3.4 Actions at the Destination SEP

The destination SEP is not expected to perform any INS routing functions. When the destination node receives an *XUDT* message containing the INS parameter, the received INS parameter is sent up to the SCCP User as a parameter in the N-UNITDATA indication primitive.

G.3.5 Abnormal Procedures

G.3.5.1 Actions at a INS-Capable SCCP Relay Node

If an INS-capable SCCP Relay Node receives an *XUDT* message that contains an INS parameter with the Type of Routing indicator set to "constrained routing," follows the procedures described in Item 1 of clause G.3.2.1, and determines that no route toward the derived PC (i.e., the PC derived from the NID in the received INS parameter) is available, the SCCP Relay Node will fail the message and follow the procedures described in clause G.4.

If an INS-capable SCCP Relay Node receives an *XUDT* message that contains an INS parameter with the Type of Routing indicator set to "suggested routing," follows the procedures described in Item 2 of clause G.3.2.1, and determines that no route toward the derived PC (i.e., the PC derived from the first NID in the received INS parameter) is available, the SCCP Relay Node will change the Type of Routing

---

[28] A non-INS-capable node is one that is unable to parse and interpret the information in the INS parameter. A non-INS-capable SCCP Relay Node may or may not be capable of recognizing the *XUDT* message.

indicator to "neither constrained nor suggested," and route the message based on the PC that resulted from the GTT performed on the received TT and GTA information. If there is no route available toward the PC that results from the GTT being performed, the SCCP Relay Node will fail the message and follow the procedures described in clause G.4. If there is no route available toward the PC that is derived from the second NID in the received INS parameter, the SCCP Relay Node will fail the message and follow the procedures described in clause G.4.

G.3.6 Error Conditions

In addition to the abnormal conditions described in clause 6.3.5, the following error conditions, which are specific to INS routing, would cause the error handling procedures described in clause G.4 to be invoked.

- An invalid INS routing request (e.g., network specific routing error) is received.

Other non-INS-specific problems such as a hop counter violation, unauthorized message or message incompatibility would also invoke SCCP error handling procedures.

G.4 Error Handling Procedures

When an *XUDT* message fails due to the conditions described above, the message return function will be initiated, if requested. The purpose of the message return function is to return an *XUDTS* message indicating that a message has encountered routing failure and cannot be delivered to its final destination. The procedure may be initiated, for example, as a result of insufficient translation information or the inaccessibility of a subsystem or Point Code.

If the undeliverable message is an *XUDT* message, and the optional field is set to "return message on error," then an *XUDTS* message is transferred to the SCCP Calling Party Address. (If the message is originated locally, an N-NOTICE indication primitive is invoked.) If the undeliverable *XUDT* message contains an INS parameter, and the SCCP Relay node at which the routing failure occurs is INS-capable, the SCCP Relay node deletes any unused INS information, sets the Type of Routing indicator to "constrained," and applies INS constrained routing procedures, as described in Item 1 of clause 3.3.2.1, to the remaining INS information with the following modifications. When the SCCP Relay Node determines whether the "next" NID identifies the network in which the current SCCP Relay Node resides, it is looking at the last NID that was used to route the *XUDT* message in the forward direction (i.e., the “counter value” NID, rather than the “counter value + 1” NID). Once an NID is used in routing the *XUDTS* message, the counter is decremented, rather than incremented. If the counter value is zero (i.e., all of the information has been used), the *XUDTS* is routed based on the Called Party Address (i.e., the Calling Party Address of the *XUDT* message).

As described in clause 4.2 of ATIS-1000112.4, if the undeliverable message is an *XUDT* message and the option field is not set to "return message on error," or if the undeliverable message is an *XUDTS* message, then the message is discarded.

G.5 Procedures for Deriving the XUDTS *Message*

The node initiating the message return function should code the *XUDTS* message as described in ATIS-1000112.3, with the following modification: Return Cause field will contain value 11111000 "invalid INS routing request" as the reason for the message return in the case of an INS routing failure.

G.6 SDL

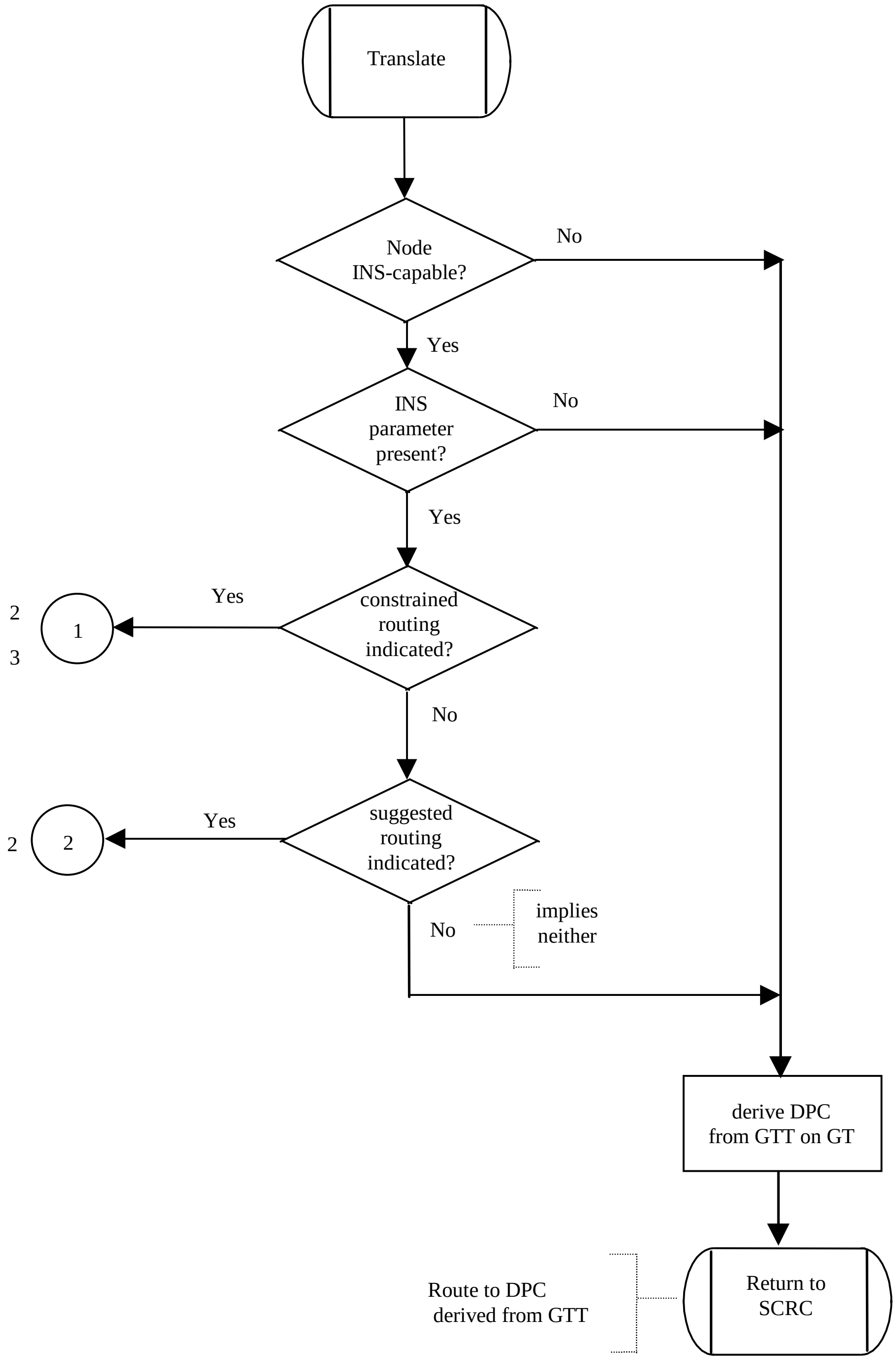


Figure G-2/ATIS-1000112.4 - Intermediate Network Selection (Sheet 1 of 4)

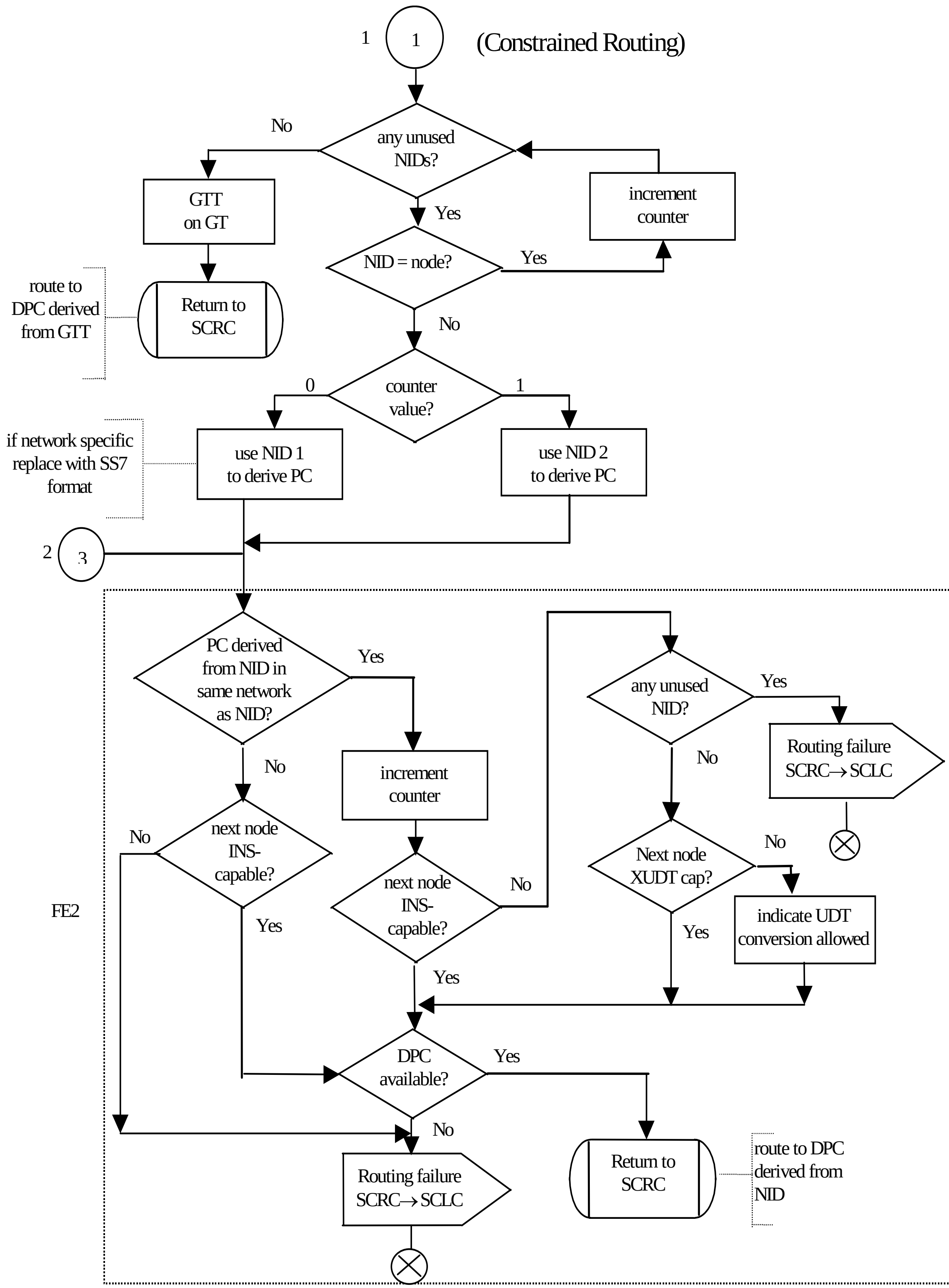


Figure G-2/ATIS-1000112.4 - Intermediate Network Selection (Sheet 2 of 4)

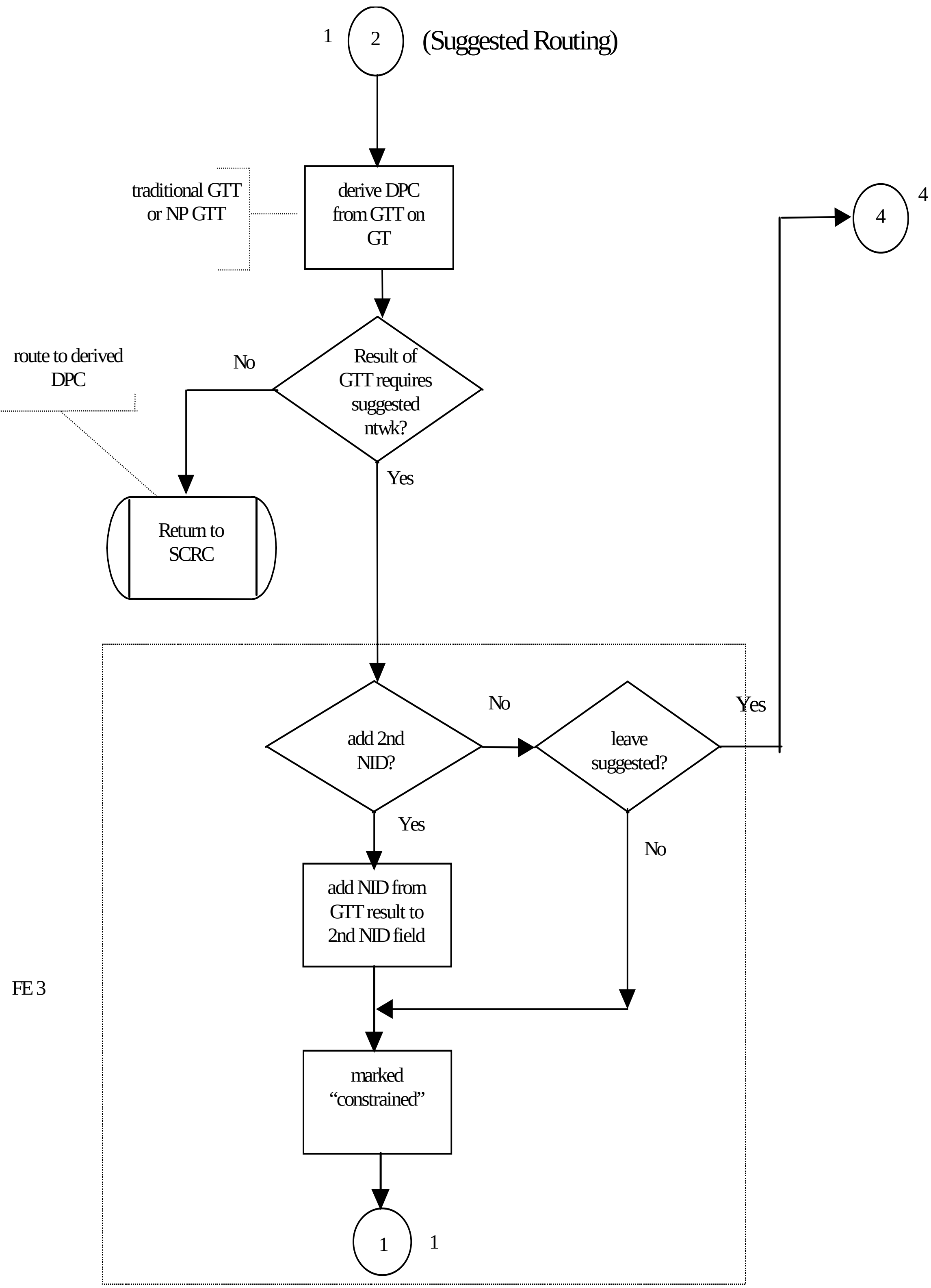


Figure G-2/ATIS-1000112.4 - Intermediate Network Selection (Sheet 3 of 4)

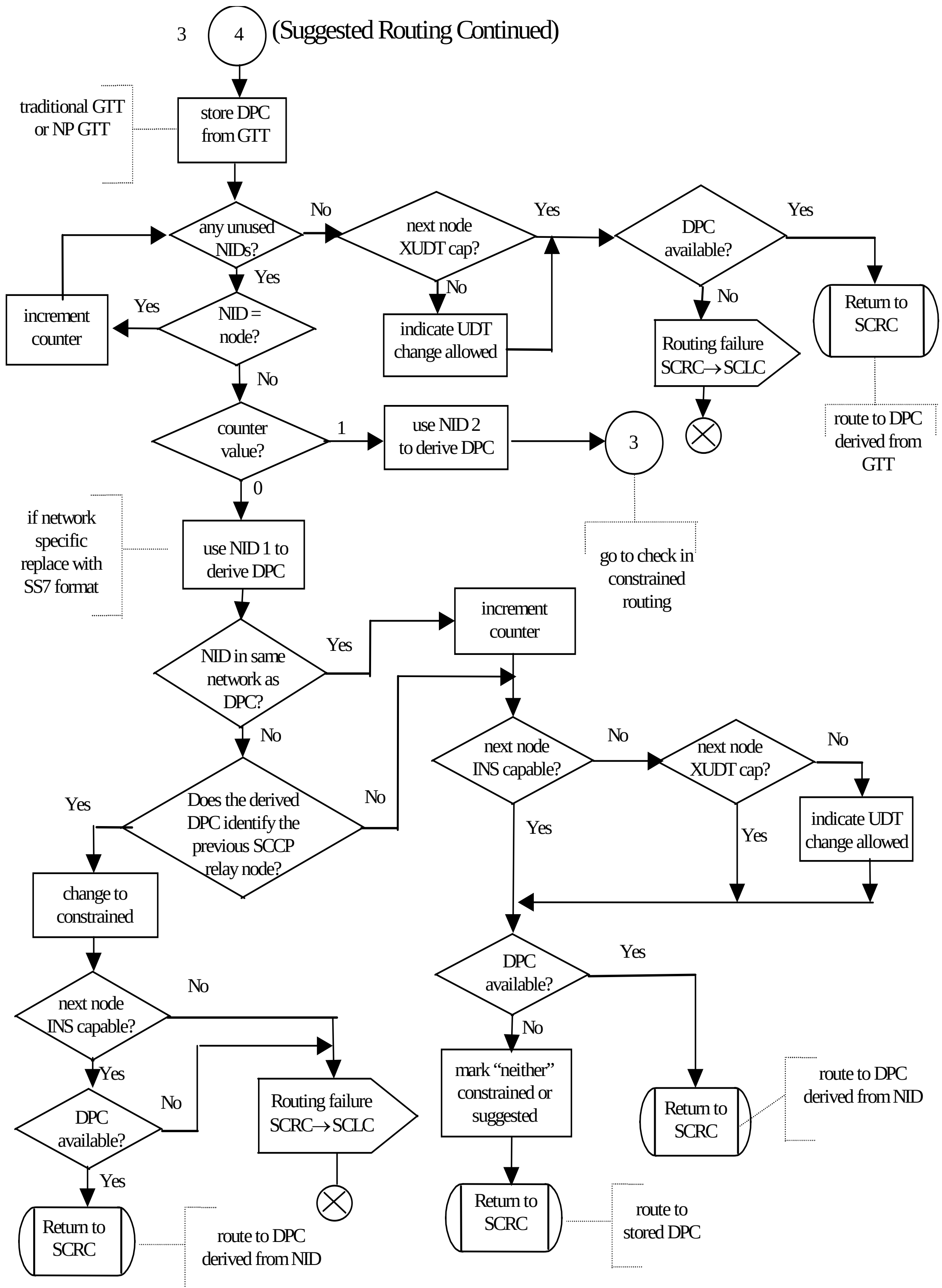


Figure G-2/ATIS-1000112.4 - Intermediate Network Selection (Sheet 4 of 4)

ATIS-1000112.5.2005

[Revision of T1.112.5-2001]

Chapter 5
Signaling Connection Control Part Performances

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

American National Standard for Telecommunications –

Signaling Connection Control Part Performances

1 SCOPE, PURPOSE, AND APPLICATION

1.1 Overview

The Signaling Connection Control Part (SCCP) of Signaling System No. 7 (SS7) is designed as a general message transport system common to the various subsystems which are using its services.

The SCCP must satisfy the requirements of these various subsystems and therefore the most stringent subsystem requirements are considered when defining a value for a performance parameter (most stringent at the time of the specification). To this end, the requirements of ISDN-User Part, the Operations, Maintenance and Administration Part (OMAP), and the dialog between an exchange and a Service Control Point (using the Transaction Capabilities) were specifically investigated. It is assumed that an SCCP that satisfies the requirements of these users mentioned above will also meet those of future users.

SCCP performances are defined by parameters of two kinds:

- Quality of Service (QoS) parameters as seen by a user of the SCCP; and
- Internal parameters that are not seen by the user but which contribute to a quality of service parameter (for example the transfer delay in a relay point, which contributes to the total transit delay of messages as seen by the user).

The definitions of all these parameters are presented in clause 2 of this chapter. Then the values allowed for the internal parameters are defined in clause 3.

1.2 Definitions

Two concepts must be defined when dealing with SCCP performances: SCCP route and SCCP relation. These concepts are similar to the one defined for the MTP (i.e., signaling route and signaling relation). They are defined as follows:

- *SCCP route*: An SCCP route is composed of an ordered list of nodes where the SCCP is used -- origin, relay(s), destination -- for the transfer of SCCP messages from an originating SCCP user to the destination SCCP user; and
- *SCCP relation*: An SCCP relation is a relation between two SCCP users that allows them to exchange data over it. An SCCP relation can consist of one or several SCCP routes.

Five types of nodes where SCCP functions are involved are defined as follows:

- Originating node (origin of a UDT/XUDT message or of a signaling connection);
- Destination node (destination of a UDT/XUDT message or of a signaling connection);

- ♦ Relay point (signaling point where the translation functions of the SCCP for connectionless classes are implemented);
- ♦ Relay point without coupling (signaling point where the relay functions of the SCCP connection-oriented classes, but without the coupling of signaling connection sections function, are implemented); and
- ♦ Relay point with coupling (signaling point where the relay functions of the SCCP connection-oriented classes, including the coupling of signaling connection sections function, are implemented).

2 DEFINITION OF PERFORMANCE PARAMETERS

Some parameters which are defined in this clause cannot be measured from the outside of a signaling point and therefore no values are attributed to them in clause 3 where only measurable values are given. This is true for some internal parameters -- for example, the transit time of a CR message for the relay function at a relay point without coupling; this parameter does not include in this definition the time due to the MTP and therefore in clause 3 values are given to the transit time at a relay point which includes both the time spent in the SCCP and the MTP.

In networks containing implementations from a number of different vendors, it may be necessary where a parameter has a send and receive component to specify that parameter on such a basis. This will then ensure the overall requirement is satisfied.

2.1 Performance Parameters for the Connectionless Classes.

2.1.1 Quality of Service Parameters

The following parameters define the QoS as seen by a user of the connectionless classes of the SCCP:

1. *Undetected errors*: This parameter gives the probability that a UDT message is delivered with user data which is defective.
2. *Residual error probability*: This parameter gives the probability that a UDT message is lost, duplicated, or delivered incorrectly by the set constituted of SCCP and the MTP (called Network Service Layer or NSL). An incorrectly delivered UDT is one in which the user data are delivered in a corrupted condition (see undetected errors above), or the user data are delivered to an incorrect NSL.

   For class 1 only, a UDT message is considered as incorrectly delivered if it is delivered out of sequence by the NSL.
3. *Out of sequence probability*: This parameter gives the probability that UDT messages are delivered out of sequence to the user by the NSL.

   NOTE - This parameter is relevant only for class 1.
4. *Total transit delay of a UDT message*: This parameter is the elapsed time between an N-UNITDATA request issued by an SCCP user at the originating node and the corresponding N-UNITDATA indication issued to the SCCP user at the destination node.

   This parameter is composed of several internal parameters:

a. Sending time of a UDT message by the SCCP;

b. MTP overall transfer time;

c. Transit time of a UDT message for the relay function at a relay point; and

d. Receiving time of a UDT message by the SCCP.

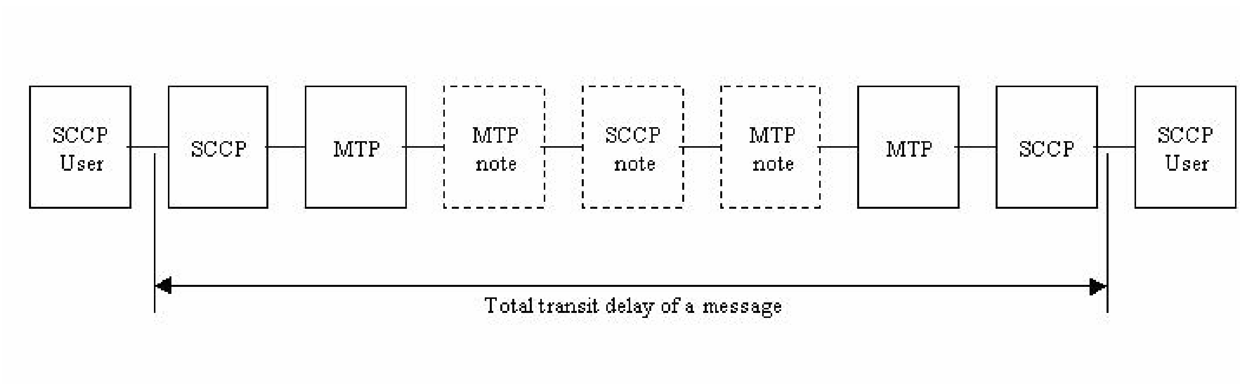
Depending on the configuration, the second parameter could appear one or several times and the third parameter could appear zero, one, or several times. This is illustrated in Figure 1/ATIS-1000112.5.

A probabilistic approach has to be taken to give values to this parameter, considering the various possible SCCP routes and the existence of queues at several points.

5. *Unavailability of an SCCP relation*: This parameter characterizes the unavailability for two SCCP users to communicate via the NSL.

   This parameter is determined by the unavailability of the individual components of an SCCP relation: SCCP at the two endpoints; one or several signaling relations; and zero, one, or several relay points.

   This unavailability can be reduced by the duplication of routes at the SCCP level.



NOTE - Zero, one, or several relay points can be present depending on the network configuration.

Figure 1/ATIS-1000112.5 - Functional Diagram of the Total Transit Delay of a Message

2.1.2 Internal Parameters

The following parameters are internal to the network service, but they contribute to the QoS as components of a parameter of the previous clause for connectionless classes of the SCCP.

1. *Sending time of a UDT message by the SCCP*: This parameter is the elapsed time between an N-UNITDATA request and the corresponding MTP TRANSFER request at the originating node.

   NOTE - The value of this parameter may differ substantially depending on whether or not a translation function is used in the SCCP.

2. *MTP overall transfer time*: This parameter is already defined in Chapter ATIS-1000111.6 as parameter T0 in clause 4.3.3.

3. *Transit time of a UDT message for the relay function at a relay point*: This parameter is the elapsed time between an MTP-TRANSFER indication primitive corresponding to an incoming UDT

message at a relay point (i.e., a signaling point where is implemented the SCCP translation functions are implemented), and the associated MTP-TRANSFER request primitive corresponding to the outgoing UDT message (which may differ from the incoming one by the called party address).

A probabilistic approach has to be taken to give values to this parameter, considering the existence of queues and that it is possible for the translation functions to be congested.

4. *Receiving time of a UDT message by the SCCP*: This parameter is the elapsed time between an MTP-TRANSFER indication and the corresponding N-UNITDATA indication at the destination node.

5. *Unavailability of a relay point*: This parameter characterizes the unavailability of the translation functions of the SCCP at a relay point.

2.2 Performance Parameters for the Connection-Oriented Classes

2.2.1 Quality of Service Parameters

The following parameters define the QoS as seen by a user of the connection-oriented classes of the SCCP:

1. Signaling connection establishment time: This parameter is the elapsed time between an N-CONNECT request primitive and the corresponding N-CONNECT confirmation primitive for a successful signaling connection establishment.

   This delay is composed of two parameters: one which depends on the user at the destination node and one which depends on the NSL. The first one, which is the elapsed time between an N-CONNECT indication and response at the destination, will be specified for each user. The second one is an internal parameter of the SCCP and will be called the SCCP component of the signaling connection establishment time. It will be specified in this SCCP performances chapter.

   Moreover it is possible to specify here the maximum signaling connection establishment time. It is equal to the connection establishment timer (see Chapter ATIS-1000112.4).

2. *Signaling connection establishment failure probability*: A signaling connection establishment failure is defined as a connection refusal or a time-out for the connection establishment timer coming from the SCCP.

   The dimensioning of the SCCP regarding the number of local reference numbers will impact this signaling connection establishment failure probability. The unavailability of an SCCP relation is also an internal parameter impacting this probability.

   The connection refusals coming from the called user must not be taken into account. This also applies for the time-out coming from this called user.

   NOTE - It is possible for the connection refusals to distinguish between the one coming from the user and the one coming from the SCCP, but that is impossible for the time-out of the connection establishment timer.

3. *Throughput*: This parameter is specified independently for each direction of transmission and corresponds to a number of octets of user data (contained in NSDU) transferred per second on a signaling connection.

   NOTE - Only successfully transferred user data are taken into account, which means data that are transferred to the correct destination, error free, and without missequencing.

4. *Overall transit time of DT messages*: This parameter is the elapsed time between an N-DATA request and the corresponding N-DATA indication.

   This parameter is composed of several internal parameters:

   a. Sending time of a DT message by the SCCP;
   b. MTP overall transfer time;
   c. Transit time of a DT message for the relay function at a relay point with coupling; and
   d. Receiving time of a DT message by the SCCP.

   Depending on the configuration of the signaling connection, the second parameter could appear one or several times and the third parameter could appear zero, one, or several times (see Figure 1/ATIS-1000112.5).

   A probabilistic approach has to be taken to give values to this parameter, considering the various possible SCCP routes and the existence of queues at several points.

5. *Undetected errors*: This parameter gives the probability that a DT message is delivered with user data which is defective.

6. *Residual error rate for DT messages*: This parameter gives the probability that a DT message is lost, duplicated, missequenced, or incorrectly delivered by the NSL.

   A DT message is incorrectly delivered if user data is delivered in a corrupted condition (see undetected errors above), or the user data are delivered to an incorrect NSAP.

7. *Out of sequence probability for DT messages*: This parameter gives the probability that DT messages are delivered out of sequence to the user by the NSL.

8. *Signaling connection unsolicited reset and premature release probability*: This parameter gives the probability that a connection release or reinitialization due to the SCCP occurs on a signaling connection during a given time.

   The unavailability of an SCCP relation is an internal parameter to be considered when calculating the probability of a connection release occurrence due to the SCCP.

9. *Signaling connection reset delay*: This parameter is the elapsed time between an N-RESET request primitive and the corresponding N-RESET confirmation primitive for a successful signaling connection reset.

2.2.2 Internal Parameters

The following parameters are internal to the network service, but they contribute to the QoS as components of a parameter of the previous clause for connection-oriented classes of the SCCP.

1. *SCCP component of the signaling connection establishment time*: This parameter is composed of two times:

   - ♦ The elapsed time between an N-CONNECT request primitive at the origin node and the corresponding N-CONNECT indication primitive at the destination node.
   - ♦ The elapsed time between an N-CONNECT response primitive at the destination node and the corresponding N-CONNECT confirmation primitive at the origin node.

   It is composed of several internal parameters:

   a) Sending time of a CR message by the SCCP;

b) MTP overall transfer time;

c) Transit time of a CR message for the relay function at a relay point without coupling;

d) Transit time of a CR message for the relay function at a relay point with coupling;

e) Receiving time of a CR message by the SCCP;

f) Sending time of a CC message by the SCCP;

g) Transit time of a CC message for the relay function at a relay point with coupling; and

h) Receiving time of a CC message by the SCCP.

Depending on the configuration, these parameters can appear zero, one, or several times.

A probabilistic approach has to be taken to give values to this parameter, considering the various possible configurations and the existence of queues at several points.

2. *Sending time of a CR message by the SCCP*: This parameter is the elapsed time between an N-CONNECT request primitive and the corresponding MTP-TRANSFER request primitive (for the transfer of the CR message).

   NOTE - The value of this parameter may differ substantially depending on whether or not a translation function is used in the SCCP.

3. *MTP overall transfer time*: This parameter is already defined in Chapter ATIS-1000111.6 as parameter T0 in clause 4.3.3.

4. *Transit time of a CR message for the relay function at a relay point without coupling*: This parameter is the elapsed time between an MTP-TRANSFER indication primitive corresponding to an incoming CR message at a relay point without coupling, and the associated MTP-TRANSFER request primitive corresponding to the outgoing CR message.

5. *Transit time of a CR message for the relay function at a relay point with coupling*: This parameter is the elapsed time between an MTP-TRANSFER indication primitive corresponding to an incoming CR message at a relay point with coupling, and the associated MTP-TRANSFER request primitive corresponding to the outgoing CR message (which may differ from the incoming one only by the called party address).

6. *Receiving time of a CR message by the SCCP*: This parameter is the elapsed time between an MTP-TRANSFER indication primitive (for an incoming CR message), and the corresponding N-CONNECT indication primitive.

7. *Sending time of a CC message by the SCCP*: This parameter is the elapsed time between an N-CONNECT response primitive and the corresponding MTP-TRANSFER request primitive (for the transfer of the CC message).

8. *Transit time of a CC message for the relay function at a relay point with coupling*: This parameter is the elapsed time between an MTP-TRANSFER indication primitive corresponding to an incoming CC message at a relay point with coupling, and the associated MTP-TRANSFER request primitive corresponding to the outgoing CC message.

9. *Receiving time of a CC message by the SCCP*: This parameter is the elapsed time between an MTP-TRANSFER indication primitive (for an incoming CC message), and the corresponding N-CONNECT confirmation primitive.

10. *Unavailability of an SCCP relation*: This parameter characterizes the unavailability for two SCCP users to communicate via the NSL.

This parameter is determined by the unavailability of the individual components of an SCCP relation: the SCCP at the two endpoints, one or several signaling relations and zero, one, or several relay points with coupling and without coupling.

This unavailability can be reduced by the duplication of routes at the SCCP level.

11. *Unavailability of a relay point*: This parameter characterizes the unavailability of the SCCP at a relay point.
12. *Sending time of a DT message by the SCCP*: This parameter is the elapsed time between an N-DATA request primitive and the corresponding MTP-TRANSFER request primitive (for the transfer of a DT message).
13. *Transit time of a DT message for the relay function at a relay point with coupling*: This parameter is the elapsed time between an MTP-TRANSFER indication primitive corresponding to an incoming DT message at a relay point with coupling, and the associated MTP-TRANSFER request primitive corresponding to the outgoing DT message.
14. *Receiving time of a DT message by the SCCP*: This parameter is the elapsed time between an MTP-TRANSFER indication primitive (for an incoming DT message), and the corresponding N-DATA indication primitive.

2.3 Correspondence between the QoS Parameters and the Class.

The correspondence between the QoS parameters defined above, in clauses 2.1.1 and 2.2.1, and their applicability to the various classes of the SCCP is illustrated in Table 1/ATIS-1000112.5 below:

Table 1/ATIS-1000112.5 - Applicability of QoS Parameters to SCCP Classes

PARAMETER	CLASSES			
	0	1	2	3
Undetected errors	X	X	X	X
Residual error probability	X	X	X	X
Out of sequence probability		X	X	X
Total transit delay of a message	X	X	X	X
Unavailability of an SCCP relation	X	X	X	X
Signaling connection establishment time			X	X
Signaling connection establishment failure probability			X	X
Throughput			X	X
Signaling connection unsolicited reset and parameter release probability			X	X
Signaling connection reset delay				X

3 SPECIFIED VALUES FOR INTERNAL PARAMETERS

3.1 Internal Parameters for Classes 0 and 1

1. *Transit time of a UDT message in a relay point*: The transit time of a UDT message in a relay point is composed of the transit time of a UDT message for the relay function at a relay point, and of the time elapsed in the MTP at this relay point for the UDT message; it is measurable externally. It is described in Figure 2/ATIS-1000112.5 and it should not exceed the values given in Table 2/ATIS-1000112.5:

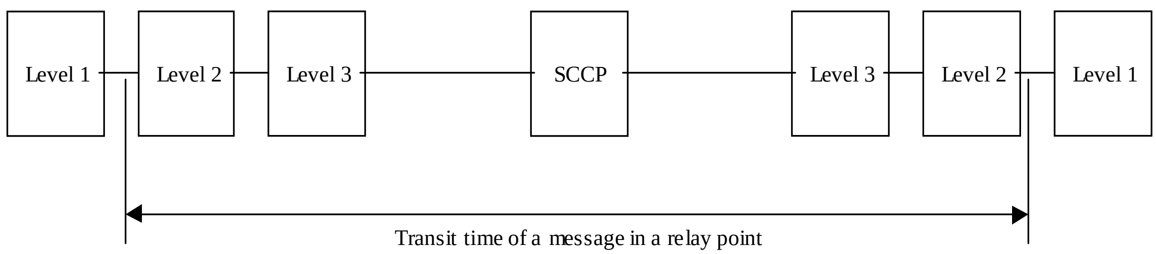


Figure 2/ATIS-1000112.5 - Functional Diagram for the Transit Time of a Message in a Relay Point

Table 2/ATIS-1000112.5 - Allowable Transit Time as a Function of Translation Function Traffic Load (UDT Message)

Traffic load for the translation function	Transit time of a UDT message in a relay point (in ms)	
	Mean	95%
Normal	50 - 155	100 - 310
+ 15%	100 - 233	200 - 465
+ 30%	250 - 388	500 - 775

NOTE - All values are provisional.

The normal traffic load for the translation function is the load for which the point is dimensioned.

These figures assume a message length distribution as given in Table 2/ATIS-1000111.6 (short messages with a mean message length of 120 bits). For long messages (272 octets of SIF), it is necessary to add about 30 ms to each figure, to take into account the emitting time at 64 Kbit/s --much longer for long messages than for short messages.

2. *Unavailability of a relay point*: The unavailability of a relay point should not exceed 10^{-4}.

3.2 Internal Parameters for Classes 2 and 3

1. *Transit time of a CR message in a relay point without coupling*: The transit time of a CR message in a relay point without coupling is composed of the transit time of a CR message for the relay function at a relay point without coupling, and of the time elapsed in the MTP at this relay point without coupling for the CR message; it is measurable externally. It should not exceed the following values:

Table 3/ATIS-1000112.5 - Allowable Transit Time (Relay Point without Coupling) as a Function of Relay Function Traffic Load (CR Message)

Traffic load for the relay function	Transit time of a CR message in a relay point without coupling (in ms)	
	Mean	95%
Normal	50 - 155	100 - 310
+ 15%	100 - 233	200 - 465
+ 30%	250 - 388	500 - 775

NOTE - All values are provisional.

The normal traffic load for the relay function is the load for which the point is dimensioned.

These figures assume a message length distribution as given in Table 2/ATIS-1000111.6 (short messages with a mean message length of 120 bits). For long messages (128 octets of SCCP user data), it is necessary to add about 15 ms to each figure, to take into account the emitting time at 64 Kbit/s -- much longer for long messages than for short messages.

2. *Transit time of a CR message in a relay point with coupling*: The transit time of a CR message in a relay point with coupling is composed of the transit time of a CR message for the relay function at a relay point with coupling, and of the time elapsed in the MTP at this relay point with coupling for the CR message; it is measurable externally. It should not exceed the following values:

Table 4/ATIS-1000112.5 - Allowable Transit Time (Relay Point with Coupling) as a Function of Relay Function Traffic Load (CR Message)"

Traffic load for the relay function with coupling	Transit time of a CR message in a relay point without coupling (in ms)	
	Mean	95%
Normal	75 - 180	150 - 360
+ 15%	150 - 270	300 - 540
+ 30%	375 - 450	750 - 900

NOTE - All values are provisional.

The normal traffic load for the relay function is the load for which the point is dimensioned.

These figures assume a message length distribution as given in Table 2/ATIS-1000111.6 (short messages with a mean message length of 120 bits). For long messages (128 octets of SCCP user data), it is necessary to add about 15 ms to each figure, to take into account the emitting time at 64 Kbit/s -- much longer for long messages than for short messages.

3. *Transit time of a CC message in a relay point with coupling*: The transit time of a CC message in a relay point with coupling is composed of the transit time of a CC message for the relay function at a relay point with coupling, and of the time elapsed in the MTP at this relay point with coupling for the CC message; it is measurable externally. It should not exceed the following values:

Table 5/ATIS-1000112.5 - Allowable Transit Time (Relay Point with Coupling) as a Function of Relay Function Traffic Load (CC Message)

Traffic load for the relay function with coupling	Transit time of a CC message in a relay point without coupling (in ms)	
	Mean	95%
Normal	30 - 110	60 - 220
+ 15%	60 - 165	120 - 330
+ 30%	150 - 275	300 - 550

NOTE - All values are provisional.

The normal traffic load for the relay function is the load for which the point is dimensioned.

These figures assume a message length distribution as given in Table 2/ATIS-1000111.6 (short messages with a mean message length of 120 bits). For long messages (128 octets of SCCP user data), it is necessary to add about 15 ms to each figure, to take into account the emitting time at 64 Kbit/s -- much longer for long messages than for short messages.

4. *Transit time of a DT message in a relay point with coupling*: The transit time of a DT message (DT1 or DT2) in a relay point with coupling is composed of the transit time of a DT message for the relay function at a relay point with coupling, and of the time elapsed in the MTP at this relay point with coupling for the DT message; it is measurable externally. It should not exceed the following values:

Table 6/ATIS-1000112.5 - Allowable Transit Time (Relay Point with Coupling) as a Function of Relay Function Traffic Load (DT Message)

Traffic load for the relay function with coupling	Transit time of a DT message in a relay point without coupling (in ms)	
	Mean	95%
Normal	30 - 110	60 - 220
+ 15%	60 - 165	120 - 330
+ 30%	150 - 275	300 - 550

NOTE - All values are provisional.

The normal traffic load for the relay function is the load for which the point is dimensioned.

These figures assume a message length distribution as given in Table 2/ATIS-1000111.6 (short messages with a mean message length of 120 bits). For long messages (255 octets of SCCP user data), it is necessary to add about 30 ms to each figure, to take into account the emitting time at 64 Kbit/s -- much longer for long messages than for short messages.

5. *Unavailability of a relay point without coupling*: The unavailability of a relay point without coupling should not exceed 10^{-4}.

6. *Unavailability of a relay point with coupling*: The unavailability of a relay point with coupling is for further study.

Chapter 6
Signaling Connection Control Part Users Guide

TABLE OF CONTENTS

TABLE OF FIGURES

American National Standard for Telecommunications –

Signaling Connection Control Part Users Guide

1 SCOPE

This chapter describes guidelines for using the recommendations in ANSI SCCP protocol (ATIS-1000112.1 through ATIS-1000112.5). In addition to protocol aspects, this chapter provides guidance to specifiers of SCCP-applications and implementers on a number of issues related to the incorporation of SCCP into their networks. The following topics are currently included in this chapter:

1. *Compatibility Issues*: Differences among the versions of the SCCP standard and discussions on co-operation between implementations of the different versions of the standard are addressed.
2. *SCCP Addressing and Routing*: The meaning and use of addressing parameters as they relate to addressing and routing in the SCCP layer are discussed.
3. *SCCP Networking Aspects*: The network structures that may be created using the SCCP management procedures are explored. Issues related to connectionless and connection-oriented services are also addressed. Interworking issues between MTP networks supporting 272-octet messages and supporting 4095-octet messages are discussed.

This document is for guidance purposes only. It is not intended to extend, restrict, or modify the normative clauses in ATIS-1000112.1 through ATIS-1000112.5. If a discrepancy arises, the normative clauses take precedence.

2 COMPATIBILITY ISSUES

Several changes have been made to the SCCP standard from version to version. The purpose of this chapter is to record these changes and mention any interworking problems that might arise.

2.1 Differences between T1.112-1992 and T1.112-1996

This clause identifies parameters, procedures, and information that were added to or modified in T1.112-1992 to create T1.112-1996.

2.1.1 Encoding for Global Title Indicator (GTI) = 0001

An encoding for Private Network or Network Specific Numbering Plan was added for GTI = 0001. See clause 3.4.2.3.1 of ATIS-1000112.3. GTI =0001 is presently not used in ANSI networks.

2.1.2 Segmentation Parameter

A four-octet segmentation parameter has been added to the list of SCCP parameters. The purpose of this parameter is to indicate that an SCCP message has been segmented. The parameter also contains all the information necessary to correctly reassemble the message. See clause 3.18 of ATIS-1000112.3 for further details.

2.1.3 Intermediate Signaling Network Identification (ISNI) Parameter

An Intermediate Signaling Network Identification parameter has been added. The detailed use of this parameter is found in the ISNI Network Capability description (T1.118-1992 (R2005)). The parameter field is used to: (1) invoke the ISNI constrained routing function at an ISNI-capable SCCP relay node; and (2) identify the networks traversed by the signaling messages. The parameter contains a list of two-octet Network Identifiers (NID); an indicator of the type of routing: constrained, suggested or neither; an indicator to request a logged record of the networks traversed by the signaling messages; a counter which is dynamically incremented to indicate which NID should be used for routing and identification; and a type indicator to indicate the format of the parameter.

2.1.4 Return Cause Parameter

The following reasons for message return have been encoded:

- Error in message transport (1);
- Error in local processing (1);
- Destination cannot perform reassembly (1);
- SCCP failure;
- SCCP hop counter violation;
- Invalid ISNI routing request (1);
- Unauthorized message;
- Message incompatibility;
- Cannot perform ISNI constrained routing (1);
- Redundant ISNI constrained routing parameter information (1); and
- Unable to perform ISNI identification (1).

(1) NOTE - only applicable to XUDTS messages.

See clause 3.12 of ATIS-1000112.3.

2.1.5 Refusal Cause Parameter

The meaning of value 00001110 has been changed from not obtained to reserved.

The following reasons for the release of a connection have been encoded:

- SCCP hop counter violation;
- SCCP failure (used by ITU-T but not by this standard);
- No translation for an address of such nature; and
- Unequipped user.

See clause 3.13 of ATIS-1000112.3.

2.1.6 SCCP Flow Control (as a part of SCCP management procedures)

This optional procedure has been added to support the suspension and resumption of SCCP traffic to a remote signaling point where the SCCP functionality has recently failed or recovered. See clause 5.5 of ATIS-1000112.4.

2.1.7 SCCP Restart

When a signaling point has restarted, an indication from the MTP to the SCCP is sent to tell which signaling points are accessible after restart. This procedure was added in T1.112-1996. See clause 5.6 of ATIS-1000112.4

2.1.8 Segmentation/Reassembly (for connectionless procedures)

T1.112-1996 defines a procedure called segmentation that may be used depending on the length of the user data. If segmentation is performed, the original data is broken into smaller blocks of user data and each block is sent in an XUDT. A process for reassembling the data at the destination node is also described. Clause 4.1.1 of ATIS-1000112.4 contains details on the procedure.

2.1.9 Compatibility and handling of Unrecognized messages

T1.112-1996 requires that all implementations be able to recognize all the messages in each of the protocol classes. As a result, procedures for handling unrecognized messages or parameters, unsupported optional parameters, gaps, and the treatment of spare fields have all been defined in clause 1.1.4 of ATIS-1000112.4-96.

2.1.10 Connection Refusal (in connection-oriented procedures)

T1.112-1996 defines procedural differences for connection refusal depending on where it is initiated (i.e., at the destination, origination, or relay node). Clause 3.2 of ATIS-1000112.4 describes the details of this procedure.

2.1.11 SCCP Reaction to Local MTP Restart

SCCP management procedures for the receipt of an indication of the end of an MTP Restart have been defined. See clause 5 of ATIS-1000112.4.

2.1.12 SCCP Accessible and Inaccessible

Procedures for local broadcasts of SCCP accessible and inaccessible have been defined. See clause 5.3.6.7-8 of ATIS-1000112.4.

2.1.13 Extended Unitdata Message (XUDT) and Extended Unitdata Service Message (XUDTS)

The maximum amount of data that can be transported in these messages has been changed to 251 octets (from 252). In addition two optional parameters, segmentation and ISNI, were defined.

2.1.14 Annexes in ATIS-1000112.3

Annex B in T1.112.3-1996 has become Annex A, and Annex A in T1.112.3-1996 has become Annex C. A new Annex B has been added, which describes the application/translation groups that have been assigned internetwork translation type values. The rationale for the rearrangement was that normative annexes must precede informative annexes to conform to the ANSI Style Guide.

2.1.15 Protocol Class 1

T1.112-1996 stipulates added requirements for Protocol Class 1, related to “in sequence” message delivery. See clause 4 of ATIS-1000112.4 for further details.

2.1.16 Replicated Nodes/Subsystems

SCCP management was extended in T1.112-1996 to allow for a configuration where a node/subsystem may have multiple backups operating in a mode based on preference (priority and accessibility). Each backup node is assigned a unique priority, and a combination of accessibility and priority determines which node traffic is routed to.

2.2 Differences between T1.112-1996 and T1.112-2001

2.2.1 Support of Long Message (LUDT) Capability

To support signaling for B-ISDN, an extension to the MTP level 3 has been defined. It allows the transportation of large signaling messages, via SAAL links, at potentially much higher data rates than MTP level 2. To exploit these new capabilities of the MTP within SCCP, two new message types were defined -- Long Unitdata Message (LUDT) and Long Unitdata Service Message (LUDTS) -- and one new parameter (Long Data). These messages and parameter allow the transportation of up to 3904 octets of user data without invocation of the segmentation procedures.

2.2.2 Compatibility test

A compatibility test in the SCCP Routing Control (SCRC) for connectionless procedures was initially defined in T1.112-2001. It determines whether a message needs to be segmented, truncated, or its type changed in order to be transmitted across a network boundary. This procedure was introduced to support interworking between narrowband and broadband signaling links.

2.2.3 Segmentation

Enhanced and new segmentation procedures have been defined in ATIS-1000112. In addition, two specific reasons have been defined under the return on error procedures: 1) segmentation not supported; and 2) segmentation failed. ATIS-1000112 allows segmentation in relay nodes to facilitate interworking between networks that are able to transport long messages and networks that cannot.

2.2.4 Coordinated State Change procedures

The coordinated state change procedure in ATIS-1000112 was extended. With the revision in T1.112-2001, coordinated state change is now allowed for a configuration where a node/subsystem may have multiple backups based on preference (priority and accessibility) and a configuration where a group of nodes/subsystems are operating in the loadshare mode (equal priority).

2.2.5 SCCP Loadsharing

In the context of SCCP management, ATIS-1000112 defines a loadshare mode. This mode allows traffic routed on global title to be distributed equally among a set of replicated nodes. The mechanism used by the STPs to achieve this loadsharing is implementation dependent. Procedural additions have been made to Signaling Point Status Management and Subsystem Status Management to support the loadshare mode. See clause 5 of ATIS-1000112.4.

2.3 Interworking between T1.112-1996 and T1.112-2001

2.3.1 Support of Long Message (LUDT) Capability

The introduction of the new message types, LUDT and LUDTS, potentially leads to incompatibilities because:

- ♦ These new message types are not recognized in older versions;
- ♦ The formatting rules for these messages differ from the existing SCCP messages in that all the pointers and the length field are extended to two octets; and

- The new messages may be longer than 272 octets, in which case they can only be transported if MTP capabilities supporting 4095-octet MSUs are available.

However, it is a requirement that:

- B-ISDN or other long message capable services using SCCP can also be introduced where only SCCP without enhancement to support long messages is available; and
- Other existing SCCP should be able to benefit from the new capabilities offered by MTP networks using SAAL as a level 2 protocol.

Provisions have therefore been made for *Interworking* and *Transparency*.

- *Interworking*: Since the SCRC has only limited knowledge of the transport capabilities in the SCCP network, it cannot determine whether MTP capabilities supporting 4095-octet MSUs are available end-to-end. The SCCP only has knowledge of the path to the next node. It is therefore necessary for certain interworking nodes to have the capability to convert the new message types to the types supported in T1.112-1996. This may require segmenting a LUDT into multiple XUDTs, or truncating a LUDTS message to fit into one XUDTS. The truncation of a LUDTS is allowed, as all the user data included in this message is not important when informing an originating node of a routing failure. However a LUDT must be segmented and *not* truncated if interworking is necessary, as all the user data is important to the destination node.
- *Transparency*: The service delivered to the SCCP user remains unchanged. From the viewpoint of the SCCP user, whether MTP capabilities for SAAL links are present or not is transparent. The SCCP will ensure that the correct message types are sent out.

The network operator is responsible to ensure that:

- Interworking nodes with the necessary capabilities are provided at those places where needed; and
- Support of LUDT(S) messages is consistent with the structure of the underlying MTP network and the capabilities of the SCCP node.

3 USE OF ADDRESSING PARAMETER

3.1 Scope and Purpose

SCCP addressing capabilities allow for the combination of parameters for routing in the SS7 network. This chapter provides general guidelines on when to make use of the various parameters -- such as translation types (TT), subsystem numbers (SSN) and numbering plans (NP) -- and their effect on routing in the signaling network.

3.2 Description of addressing parameters

SCCP allows two ways for the SCCP user to specify an address (either Calling Party Address or Called Party Address), namely:

1. *Global Title* - A global title (GT) consists of a global title address (GTA) -- for example, dialed digits -- and a TT, which does not explicitly contain information which could be used for routing in the SS7 network. The translation function of the SCCP is required to get the information on which routing may be done, namely a Destination Point Code (DPC) and possibly a SSN.

   With this type of addressing, routing in the network uses the global title in the Called Party Address as the address information element. The SSN, if present, does not take part in the digit translation that determines the destination node. In relay nodes, the SSN is normally passed transparently.

2. *Point Code + Subsystem Number (PC + SSN)* - A point code and a subsystem number allow for direct routing in the signaling network. The point code (PC) from the Called Party Address is used as the DPC in the MTP routing label. In the calling address (used for a reply or message return), the PC is either supplied by the Calling Party Address parameter, or if unavailable, by the Origination Point Code (OPC) in the MTP routing label.

In situations where the SCCP translation function is necessary for routing in the network, Global Title Translation (GTT) may be used. The GT information may be supplemented by optional routing parameter information, like the ISNI[1] parameter. GTT may be done in a single stage, or multiple GTTs may be required to get to the destination node. Multiple translations are required in cases where local STP tables are provisioned such that, for particular messages, routing to another STP is necessary for the intended destination to be reached.

In the cases where a reply or message return is required, the Calling Party Address plus the OPC in the routing label must contain sufficient information to clearly identify the originator of the message. If GTT is necessary for routing, the OPC will change and in such situations the Calling Party Address should not contain only the SSN but some other information on which routing can be done (e.g., PC). However, in a situation where routing on global title is done in the reverse direction (for message reply), the point code may be omitted.

3.2.1 Subsystem Number

The SSN identifies a SCCP user function (i.e., the SCCP-user) that will handle the received message. It also identifies the subsystem that is accessed via the SCCP within a node. The Point Code and the SSN, together are the addressing information that locate an application process (AP) at an SS7 node. The current list of standardized SSNs can be found in clause 3.4.2.1 of ATIS-1000112.3. Standardization of SSNs is deprecated except for specific cases (e.g., OMAP) where:

1. The subsystem can also be standardized;
2. The subsystem functionality is sufficiently narrow that any reasonable implementation will not be divisible into functions that could fail separately (requiring separate subsystem management); and

---

[1] The Intermediate Signaling Network Identification (ISNI) parameter allows a feature in the initiating network to notify the terminating network of the interconnecting CCS networks (ICNs) for non-circuit associated messages as well as specify the routing of the message. By placing the identifier(s) of the ICN(s) into the SCCP ISNI parameter, part or all of the message path to terminating Signaling End Point is described.

3. The subsystem is normally reached without GTT.

The SSN should not be used to provide addressing to individual services, features, or 'functional entities' within an AP. These items are only roles or functions within a certain AP. The distribution within an AP is usually based on the context of the received message.

3.2.2 The Global Title

The format of a GT is of variable length and may contain a TT, encoding scheme (ES), numbering plan (NP), and address information, or may simply contain a TT and the address information. The format depends on the value of the global title indicator (GTI). Figures 1 and 2 show examples of the standardized global title formats. The translation types that have been standardized are all for GTI value of 2.

3.2.2.1 Translation Type

The TT is a one-octet field that is used to direct a message to the appropriate GTT function. For the same dialed digits (e.g., a subscriber number), several translation results may be required. If this is the case, another information element must be available and the TT fulfills this requirement. Translation types are therefore to be assigned so that the different uses of the same GT digits, by different application processes, may be distinguished. A TT may imply a specific service to be provided by the SCCP-user (e.g., 800 number translation), or identify the category of service to be provided (e.g., dialed number screening or password validation). In contrast to the Numbering Plan, the TT is a purely SCCP concept.

3.2.2.1.1 Role of the Translation Type in the GTT

The TT is a value used as input to a GTT and is fundamental to SCCP routing. It identifies the type of translation required for a GTA, such as the input format or the context under which the GTA is to be interpreted.

The TT provides a means of distinguishing between the same GTA used to route to multiple, unrelated applications. For example, Calling Name Delivery (CNAM) uses the calling party number (i.e., NPA-NXX-XXXX) as the global title in the TCAP query. Similarly, Call Management applications (e.g., Automatic Callback) use the called party number (i.e., NPA-NXX-XXXX) as the global title address in the TCAP query. The same digits could be used as the global title address in a TCAP query for either of these applications. At an STP, a GTT using one TT with a particular NPA-NXX-XXXX will result in one DPC and possibly a SSN, but use of another TT could result in a different DPC and SSN for the same NPA-NXX-XXXX. In order to route messages for CNAM and Call Management applications that use the same GTA to different locations, unique TTs are assigned for each service.

Applications with the same routing needs (i.e., the same range of GTA values resulting in a translation to the same application process at the same CCS node) may use the same TT value.

3.2.2.2 Encoding Scheme

The ES parameter gives information about the coding 'syntax' (interpretation) of the GT address and as such is not a part of the address information itself. This information may be explicitly available (i.e., encoded separately) or may be inferred from the TT depending on the value of the GTI[2]. The ANSI assignments for the encoding scheme parameter (which align with ITU-T usage) may be found in clause 3 of ATIS-1000112.3.

3.2.2.3 Numbering Plan

A numbering plan is a numbering scheme for users of telecommunications services in different telecommunications networks. As an example, ITU-T Rec. E.164 for ISDN/Telephony allocates numbers for telephony subscribers, ITU-T Rec. E.212 allocates for mobile and so on. Further details about the services represented by each of the available bit sequences (in the numbering plan) may be found in clause 3.4.2 of ATIS-1000112.3.

In general numbering plans are *not* allocated by SS7, but are nevertheless referred to in ISUP, ISDN, and SCCP messages.

3.2.2.4 Global Title Indicator

The GTI tells the way in which the addressing information is formatted in the message. This indicator is encoded into bits 6543 of the address indicator. In North America, there exist two values for the global title indicator:

1. GTI = 1 includes the TT, the numbering plan, and the ES parameters. This TT is presently not used in ANSI networks and is for further study.
2. GTI = 2 includes only the TT. The information about the ES and numbering plan may be derived from the TT. This value is the same in the ITU-T Recommendations.

It should be noted that a global title indicator value of 0 is used when no global title is included. The values of 0,1,2 for the GTI are encoded in BCD format (e.g., 1 would be represented as 0001 in the bits reserved for the GTI in the address indicator).

---

[2] See clause 3.2.2.4 on Global Title Indicator.

8	7	6	5	4	3	2	1	
Translation Type								Octet 1
Numbering Plan				Encoding Scheme				Octet 2
Address Information								Octet 3 and further

Figure 1 - Global Title format for indicator 0001 (GTI = 1)

8	7	6	5	4	3	2	1	
Translation Type								Octet 1
Address Information								Octet 2 and further

Figure 2 - Global Title format for indicator 0010 (GTI = 2)

4 SCCP NETWORKING ASPECTS

4.1 Scope and Purpose

Information pertaining to both single and replicated subsystems is used for SCCP management purposes. This allows the Called Party Addresses that are specified as global titles to be translated to different point codes and/or subsystems numbers depending on the node or subsystem status. In this chapter some possible network structures that are supported by the current SCCP management capabilities will be discussed. SCCP management procedures, including their use and applicability, will then be addressed. Interworking issues as related to connectionless (and connection-oriented) services will also be explored. Finally the support of SAAL capabilities will be addressed.

4.2 Network Structures in view of SCCP management capabilities

4.2.1 Configurations of subsystems/nodes

4.2.1.1 Solitary Subsystems/Nodes

A solitary subsystem/node[3] is one that operates alone without a backup node(s) where messages can be routed in the event of a failure. Solitary nodes are the easiest to manage (compared to the variations of replicated nodes). If the destination is unavailable, SCCP management prohibits sending traffic to the node. When the node recovers, SCCP management allows the traffic to resume.

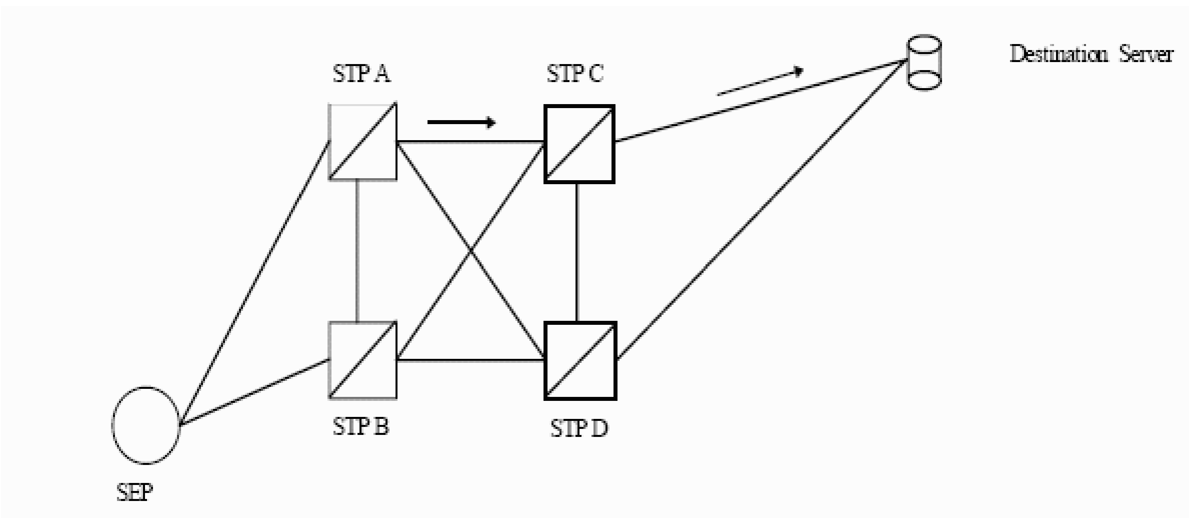


Figure 3 - Solitary Node/Subsystem

4.2.1.2 Replicated Subsystems/Nodes

When continuous availability of a service reached by SCCP routing is important (or to enhance network reliability), replication of the subsystem service may be desirable. This will ensure that subscribers will be served in the event of equipment failures, scheduled maintenance activities, physical damage to equipment site, etc.

It should be noted that T1.112-1996 prescribed an architecture of a primary and one backup node. In T1.112-2001, the limitation of having only one backup was removed. In other words, an architecture with a primary and N backups operating in the dominant mode or M replicates operating in the loadshare mode, where $N \geq 1$ and $M \geq 2$, is now allowed by the standard.

Two modes of operation that provide replication can be distinguished:

1. Dominant Mode; and

---

[3] From this point, any reference to node can be taken to mean "subsystem" also (and vice versa).

2. Loadshare Mode.

4.2.1.2.1 Dominant Mode

In the dominant mode, traffic is routed to a specific node/subsystem based on unique priorities. The priority, along with accessibility, uniquely identifies the node that particular traffic should be routed to. If a particular node becomes inaccessible, traffic is routed to the next accessible node with the highest priority (in the case of a primary/backup architecture there is only one such node). When a previously inaccessible node of higher priority (than the node now receiving the traffic) becomes available, it reassumes all the traffic.

4.2.1.2.1.1 Architecture Possibilities for the Dominant Mode

Below are several architecture possibilities for the dominant mode. The first three are for a 'pair' of nodes/subsystems, while the last two are for multiple nodes/subsystems operating in the dominant mode. This list is not intended to be exhaustive:

- Primary/Backup Pair (one passive backup serves one primary node/subsystem);
- Centralized Backup (one backup serves many primaries);
- Primary/Primary Pair (two primaries serve as backup for each other);
- Decentralized Backup (backup provision is distributed over a number of other, equally active, nodes); and
- Multiple Prioritized Backups (backup is provided by the next preferred node).

PRIMARY/BACKUP PAIR

The most obvious architecture for two replicates is the primary/backup pair. In this configuration, the primary node is active; carrying all the traffic destined for the primary/backup pair while the backup is in an idle state until it has to take over traffic due to the inaccessibility of the primary subsystem. When the primary subsystem recovers, it reassumes its normal traffic load.

In this architecture the resources needed are doubled. In this ANSI standard, the backup server may be used if the primary server is congested (see clause 5.2.4 of ATIS-1000112.4). This is presently not allowed in the equivalent ITU-T Recommendation.

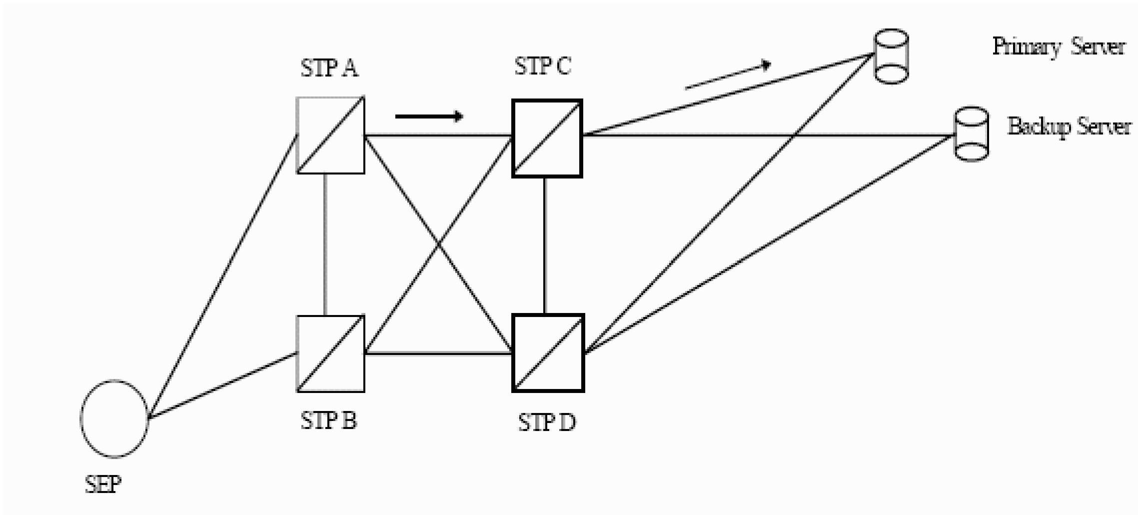


Figure 4 - Primary/Backup configuration

CENTRALIZED BACKUP

In this architecture, traffic is distributed through the administration of global title translation. Different groups of GTs are assigned a different 'primary' destination. When one of the primaries becomes inaccessible traffic is re-routed to the central backup, which must have a complete copy of the databases of all its primaries. The backup is normally idle when all the primaries are in service. This architecture is compatible with the Coordinated State Change (CSC) procedures as long as the 'dominant mode' is being used. Each primary can ask the central backup if it is ready to take over its traffic. The backup may refuse this if it is already overloaded (e.g., because it is handling the traffic of another node).

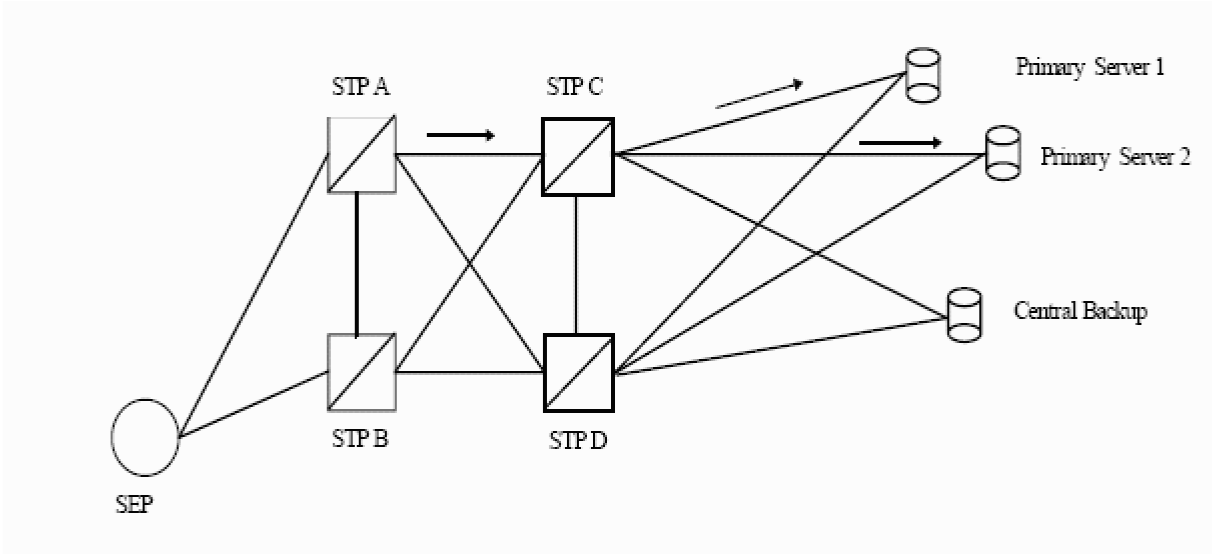


Figure 5 - Centralized Backup configuration

PRIMARY/PRIMARY PAIR

In this case, each replicate is serving a part of the traffic (e.g., each serving half). Load is distributed over the servers through administration of the GTs. For example, the GTT tables at the adjacent STP could be provisioned such that one range of GTT values goes to server 1 while another range goes to server 2, for the same service. If one server becomes inaccessible, the other server takes over the load in addition to its own. As soon as the first server resumes, traffic is redistributed again. This architecture has the advantage that the spare capacity can be used in overload situations.

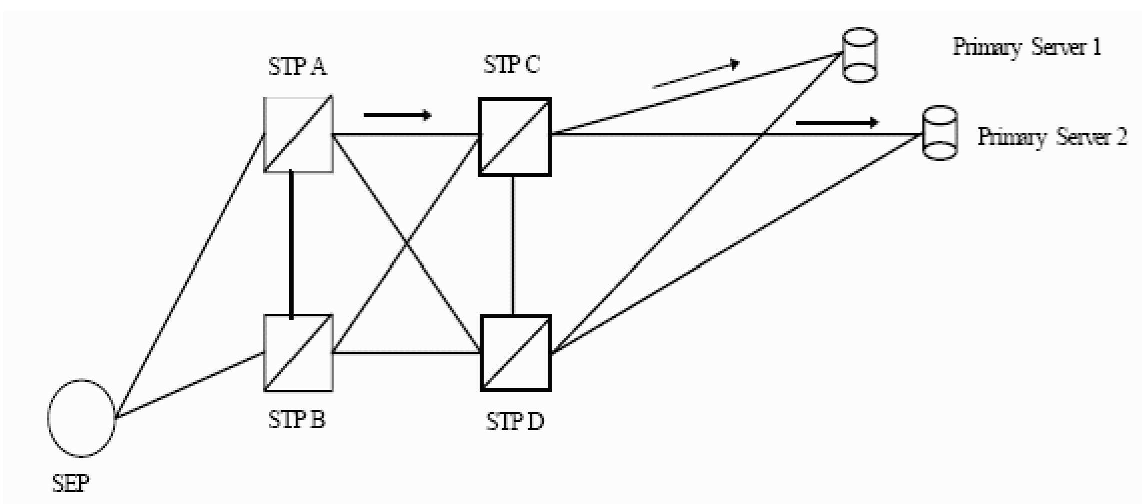


Figure 6 - Primary/Primary pair configuration

DECENTRALIZED BACKUP

It is possible to distribute the backup capability for one node by using several other nodes. This may be achieved by splitting the GTTs towards one node in groups that have the same 'primary' but multiple backups. In this case, when a primary becomes inaccessible, traffic is redistributed over the different backups such that each only handles slightly more traffic.

This architecture is not compatible with CSC procedures as it is currently defined for subsystems operating in a mode based on priorities. This system may prove, however, to be more cost efficient, since it only requires 1/N spare capacity, which is also available during overload conditions.

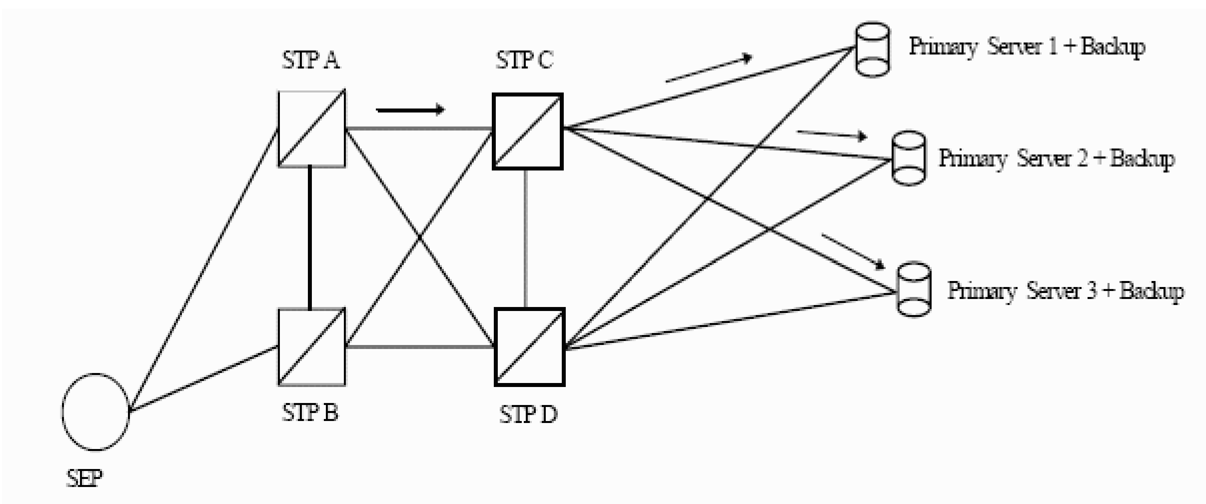


Figure 7 - Decentralized Backup configuration

MULTIPLE PRIORITIZED BACKUPS

In this architecture, each replicate is associated with a priority. The combination of priority and accessibility status of the server identifies the preferred server. At any point in time, the preferred server is the server with the highest priority that is also accessible.

Under normal conditions, traffic is routed to the node of highest priority, which is the 'preferred node.' When the current preferred node becomes inaccessible this traffic is routed to the accessible node of next highest priority, or the 'next preferred node.' Thus, the accessible node of next highest priority becomes the preferred node. Upon the recovery of a node it becomes the preferred node *if* it has a higher priority than the present preferred node (the node presently handling the traffic).

It should be noted that a server that is a priority 1 for a particular source (or GT translation) may act as a priority 2 backup for another source. This architecture may be envisioned as an extension of the Primary/Primary pair architecture. The difference is when a server become inaccessible it has more than one backup that could possibly handle its traffic, and the choice of backup is determined by priority and accessibility. Also, the spare capacity in each of the servers can be employed in overload conditions to serve more traffic.

The number of replicated nodes is limited only by practical necessity and feasibility. In the equivalent ITU-T Recommendations, the number of replicates is currently limited to two.

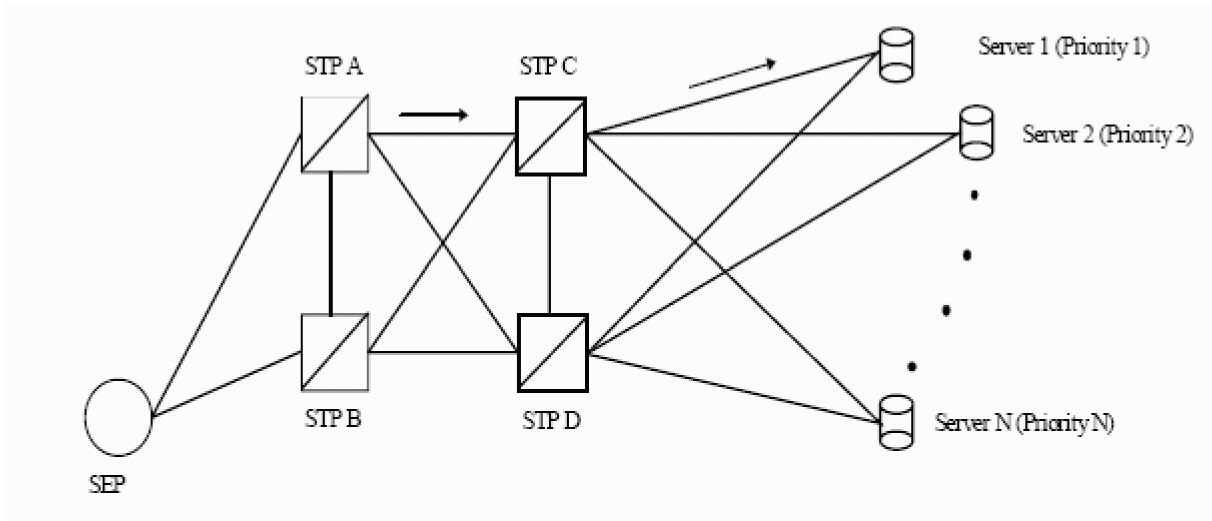


Figure 8 - Multiple Prioritized Configuration

4.2.1.2.2 Loadshare Mode

In the loadshare mode, the adjacent translator node shares the traffic equally among the N replicated nodes. The method used in the translation node to loadshare (distribute) the traffic is implementation dependent. In this mode, all the replicates are assigned equal priority and an equal portion of the traffic is handled by each of the replicated nodes. If one of the N nodes fails, that portion of the traffic is simply redistributed equally among the remaining available nodes.

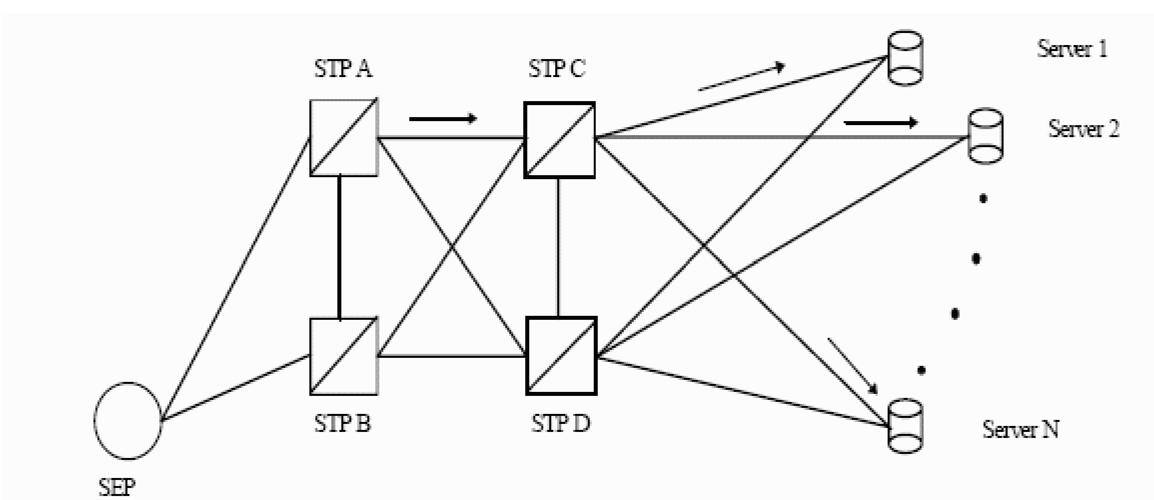


Figure 9 - SCCP Loadsharing Between N Nodes/Subsystems

4.2.1.3 Load Distribution

Load may be distributed over a number of nodes/subsystems in two ways:

1. *Static load division*: This is done by provisioning the global title translation tables such that traffic with some special characteristic(s) is routed to a particular node in a replicate set. For example, consider the sharing of 800 traffic: the GTT tables could be provisioned such that 800-0XX is routed to subsystem A and 800-5XX is routed to subsystem B. Since the load is distributed based on static information and not on actual traffic patterns, uneven distribution may result. To improve load balancing, traffic patterns could be monitored and the GTT tables manipulated regularly to obtain the desired load distribution. This is not particularly applicable to dominant mode with two replicates. Since each replicate must be designed to handle the load of both, there is little impact if the traffic mix does not lead to exactly equal loads on the two subsystems.

2. *SCCP Loadsharing*: A loadsharing mechanism that doesn't make assumptions about the frequency with which certain global titles are used (as is done in static load division) is desirable. In SCCP loadsharing, traffic is automatically distributed evenly among a set of replicates. See clause 4.2.1.2.2 for further details.

4.2.1.4 Unambiguous addresses

Whenever a replicated architecture is used, it is necessary to provide each node with its own unambiguous network address. Whereas the first message within a communication is subject to distribution, the following messages should not be. During transaction set-up, the node that is reached sends its unambiguous network address back to the message originator, which would then use it for all subsequent messages. The unambiguous network address may be in the form of a point code and SSN, or a GTT that is translated as if the solitary node architecture is being used.

4.3 SCCP Management Procedures

The purpose of SCCP management procedures is to maintain network performance by rerouting and throttling traffic in the event of network failure or congestion. SCCP management is organized into three subfunctions:

1. Signaling point status management;
2. Subsystem management; and
3. Traffic information management.

The first two subfunctions allow SCCP management to use information about the accessibility of signaling points and subsystems, respectively, so the network can adjust to failure, recovery, and congestion. Traffic information management provides SCCP users with received traffic patterns.

SCCP management procedures rely on:

1. Failure, recovery, and congestion information provided in the MTP-PAUSE, MTP-RESUME, and MTP-STATUS indication primitives; and
2. Subsystem failure, recovery, and congestion information received in SCCP management messages.

SCCP management information is currently transferred using SCCP connectionless service with no return on error requested.

4.3.1 Coordinated State Change

A replicated subsystem may be withdrawn from service by using the coordinated state change procedure, when its replicate(s) are not local. Coordinated state change can be used as follows:

1. *Primary/backup subsystem configuration*: In this case, when the primary subsystem wishes to go out of service, a SOR message is sent to the backup. The primary subsystem goes out of service when a SOG message is received from the backup subsystem.
2. *Multiple backup configuration based on priority*: In this case, a subsystem requests coordinated state change by sending a SOR message to one of its backups, and goes out of service when a SOG message is received from that backup subsystem.
3. *Loadsharing configuration*: A subsystem, in a group of subsystems, operating in the loadshare mode requests coordinated state change by sending SOR messages to all of the subsystems in the group, and goes out of service when SOG messages are received from all the subsystems.

Added details about the procedure may be found in clause 5.3.5 of ATIS-1000112.4.

4.3.2 Traffic Information Management

Traffic information management is an optional procedure that provides a mechanism whereby SCCP users may be informed of received traffic patterns. This procedure is applicable only for a subsystem with a single backup (primary/backup pair configuration). See clause 5.4 of ATIS-1000112.4 for further details.

4.4 Application of Connectionless Services

4.4.1 Connectionless Segmentation/Reassembly

With the increased need for interworking between networks that can transport long messages and networks that cannot, segmentation (and reassembly) at relay nodes have become essential. Whereas in an exclusively narrowband environment ,segmentation was unnecessary at relay nodes, in a mixed narrowband and broadband environment, segmentation at relay nodes is necessary to support SCCP messaging across network boundaries.

4.4.1.1 Segmentation

Connectionless segmentation is provided by the SCCP Connectionless Control (SCLC) block. The segmentation procedure may be initiated:

- When the SCCP generates an N-UNITDATA request primitive and the SCLC is able to segment the message before passing it the SCRC; or
- When a compatibility test in the SCRC sends a message to the SCLC for segmentation.

The actions of the SCLC is dependent on the length of the user data as follows:

1. If the length of the user data is less than X[4] octets, then segmentation should be avoided by the SCLC and a UDT, XUDT, or LUDT message should be sent;
2. If the length of the user data is between X and Y octets, then the SCLC may decide to segment the message based on locally stored information regarding network status and configuration; or
3. If the length of the user data is between Y and 3904 octets inclusive, and the SCCP decides that segmentation is necessary, then the SCCP shall segment the message. If segmentation is not possible, then the error procedure is initiated.

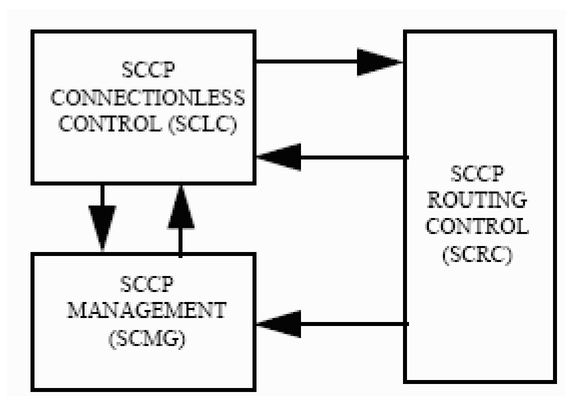


Figure 10 - SCCP Overview for connectionless services

4.4.1.1.1 Segmentation Local Reference Field

In the case where segmentation follows the reception of an LUDT message, the segmentation local reference put in each segment shall be identical to the segmentation local reference received in the segmentation parameter of the corresponding LUDT message. If the segmentation parameter was not present in the received LUDT message, then the return message option is initiated with the return cause "segmentation failure."

If segmentation is performed at a relay node, the In-Sequence Delivery Option field shall be set in each segment to the value of the protocol class received in the incoming message. This ensures that the

[4] The exact values of X and Y remain for further study.

entire message receives the treatment requested, even if SCCP segments the message simply to facilitate transport.

When an N-UNITDATA request primitive results in a single LUDT message, but there is the possibility that the message will be segmented at relay node, then the segmentation parameter should be included in the message. This simplifies segmentation at the relay node as it need not worry about changing the length of the total message because of the addition of a segmentation parameter.

4.4.1.1.2 Return on Error Procedures

If message return is requested by an SCCP user, then it is an implementation decision that determines which XUDT messages (i.e., which of the segments) have return on error requested. If an XUDTS is later received, then it also is an implementation decision that determines how the SCCP should deal with the returned XUDTS or LUDTS message.

In the case where a message has been segmented into LUDTs and return message on error is requested by the SCCP user, the return option will only be set in the first segment.

The following errors may occur during segmentation at an interworking node:

- *Segmentation non supported*: This error occurs when an LUDT arrives at an interworking node and the node is unable to perform the necessary interworking function.
- *Segmentation failed*: This error would occur when an LUDT arrives at an interworking node and the segmentation fails because of lack of resources or some transient condition in the node.

4.4.1.2 Reassembly

Upon receipt of an XUDT or LUDT message with the F-bit (i.e., the bit 8 in the first octet of the segmentation parameter which identifies whether a segment is the first in a segmented message) set to one in the segmentation parameter, the destination SCCP should initiate a new reassembly process using the Calling Part Address and Segmentation Local reference, together with the MTP routing information, to uniquely identify the reassembly process. Details of the reassembly procedures can be found in clause 4.1.1.2 of ATIS-1000112.4.

4.4.1.2.1 Return on Error Procedures

If an error occurs during reassembly, the SCCP can return an XUDTS or an LUDTS message containing the first Z (the value of Z is implementation dependent) blocks of user data received, if return on error was requested in a XUDT or the first segment of an LUDT message. For the XUDT, the decision as to which segment would contain the return on error request is implementation specific; however, in the case of the LUDT, the request for return on error must be in the first segment.

4.4.2 Message Change

When the compatibility test in the SCRC determines that the message type of an outgoing SS7 message should be different from the received message type, it requests that (because SCRC to SCLC is not an SS7 message but signaling internal to the local SCCP implementation) the SCLC change the message type; the SCLC formulates a message of the type requested by the SCRC and returns processing control to the SCRC. The information sent back to the SCRC contains *all* the information from the parameters of the message originally received by the SCLC for message type changing. This coordination between the SCLC and SCRC helps to maintain the seamless transfer of messages between networks that support different formats.

The insertion of optional parameters without message type change is permitted; their values may be network dependent. Where an optional parameter is present in a message received at an interworking node, and the resulting outgoing message is of the same type, then the optional parameter may either be deleted or its value transcribed according to the need of the outgoing network. Such parameter manipulation can also occur when the message type changes.

Where interworking between narrowband and broadband environments exists the only required format conversions are the following:

LUDT	--->	XUDT (1-N segments, message type change with or without segmentation)
LUDTS	--->	XUDTS (message type change and truncation)

The other allowed format conversions are the following (optional):

LUDT	--->	LUDT (2-N segments, no message type change but segmentation)
XUDT	--->	LUDT (message type change without reassembly)
LUDTS	--->	XUDTS (message type change without truncation)
XUDTS	--->	LUDTS (message type change without truncation)
UDT	--->	XUDT (1-N segments, message type change with or without segmentation)
XUDT	--->	UDT (message type change)
UDTS	--->	XUDTS (message type change with possible truncation)
XUDTS	--->	UDTS (message type change)

The following message format changes are to allow for interworking between different networks:

- ♦ A network may not implement XUDTs, in which case short messages would be passed as LUDTs rather than XUDTs.
- ♦ Some networks may not support XUDTs and require XUDT-to-UDT conversion. Whenever going from a “shorter” format to a “longer” format (UDT to XUDT or XUDT to LUDT), no truncation is needed or allowed.

Other format conversions are for further study.

4.4.3 Message Return

When the XUDTS message is the result of a routing failure of an LUDT message that could only be returned in an XUDTS, the user data will be cut off to fit into one XUDTS message. When the XUDTS message is the result of a routing failure of the first XUDT segment resulting from segmenting an LUDT message, the user data will contain only the first segment of data.

4.4.4 Maximal Length supported by SCCP connectionless segmentation/reassembly

MTP-2 according to ATIS-1000111.3 supports only up to 272 octet SIF-length. Due to syntax restrictions (length of a variable field is only one octet), SCCP can only send 252 octets of user data in the UDT message, or 251 in a XUDT message. This is under the condition that no GTs and optional parameters are present.

If a user wants to send longer user data, SCCP is able to transfer this using XUDT messages by segmenting the data in maximally 16 parts. The theoretically maximum amount of user data is then 3904 octets[5]. From this, the overheads for the global titles and optional parameters have to be subtracted (they are repeated in each message separately). A ‘safe’ value that the SCCP can guarantee to be possible in the foreseeable future is 2560 octets. This allows for the largest known addresses (OSI-addressing with 40 digits or 20 octets), and about 50 octets of optional parameters. Application designers should take these limits into account when fixing the syntax of application message.

When the SCCP is enhanced with long message capabilities, it can transport up to 3904 octets of user data over SAAL facilities without segmenting in one LUDT message. However, not all (parts of) the network need to provide SAAL facilities. SCCP provides interworking functions that allow a long LUDT message to be segmented into smaller parts in relay nodes and transported as XUDT messages. If the application is unsure of the availability of end-to-end SAAL links, it should put itself on the safe side and restrict the amount of user data to the safe value (i.e., 2560 octets).

4.5 Support of SAAL capabilities

4.5.1 Protocol Architecture

To support signaling for broadband and other applications with long message capabilities**,** a MTP Level 3 was defined that allows the transportation of large signaling messages via SAAL links with potentially much higher data rates than the MTP Level 2. The SCCP has been enhanced so that it can run on top of this MTP extension and optimally benefit from its new capabilities. The changes have been made in a way transparent to the SCCP-user. In this way:

- B-ISDN services using SCCP can be introduced where only the older version of SCCP is available, it is possible to later use the enhanced SCCP without any change to the application; and
- Existing SCCP users are able to benefit from the new capabilities offered by SAAL signaling links.

From the user’s point of view, there is only one SCCP. The SCCP allows the use a variety of MTP networks at the same time; two examples are shown in Figures 7 and 8.

---

[5] 3904 = (251 - 7) * 16, where 251 is the user data length that can fit into one XUDT, 16 is the maximal number of segments, and 7 the length of the optional parameter “segmentation” followed by the end of optional parameters octet.

4.5.1.1 Separate MTPs for Broadband and Narrowband

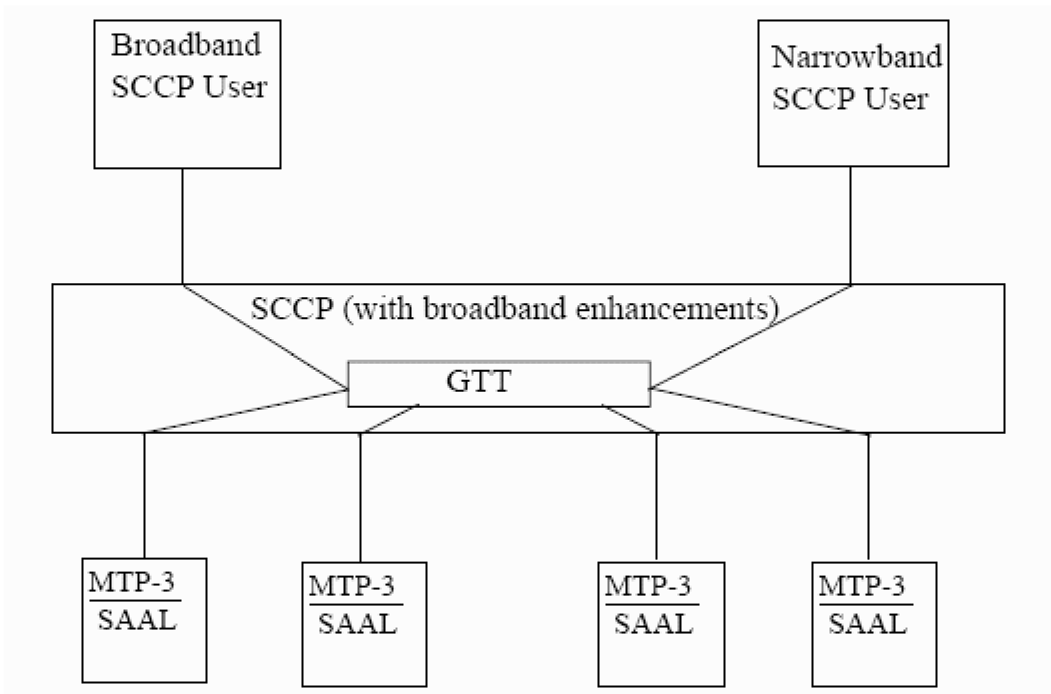


Figure 11 - Separate MTP networks for broadband and narrowband

In this scenario, the narrowband portions and broadband portions are treated as different MTP networks. Interworking occurs at the gateways where the SCCP performs a network boundary crossing.

4.5.1.2 Mixed MTP network

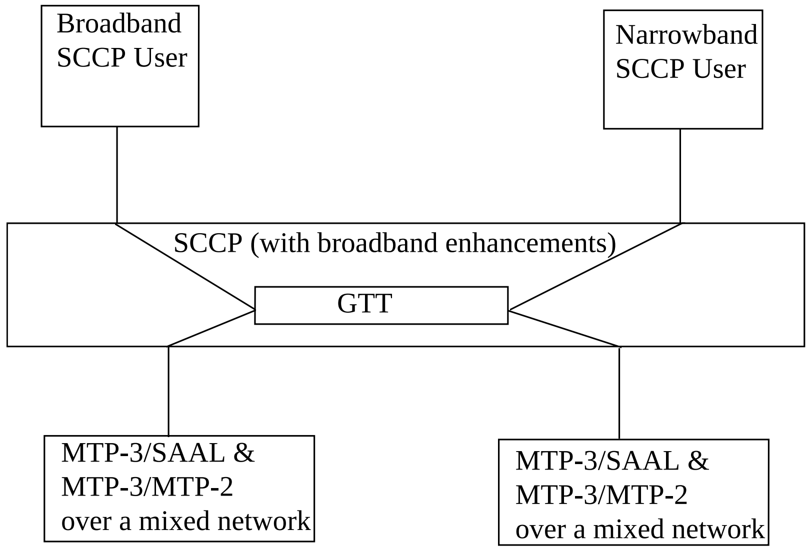


Figure 12 - Mixed broadband and narrowband network

In this architecture, mixed Broadband and Narrowband MTP exists. By mixed MTPs, it is meant that each MTP network consists of a mixture of SAAL and MTP level 2 links. The characteristics of this architecture are:

- The SCCP has the responsibility of selecting the correct MTP network over which the message would be sent out. However, SCCP cannot decide based on the local MTP alone whether it is allowed to send a long message or not, since the destination could be reachable only via narrowband links, even though initially the message was sent out from the node over a broadband link. Extra information must be stored against each destination indicating whether it is reachable via SAAL signaling links or not, and whether the destination can recognize the LUDT message type.
- In mixed MTP networks, there might be situations where a narrowband route is used as backup for a broadband route. So, whether the long message capabilities can be used or not dynamically changes. SCCP cannot know this, since it is not informed of such changes occurring at the MTP level. Therefore, it cannot always select the most optimal way to send a user-message, but must assume the worst case.

4.5.2 Interworking

From the point of view of the SCCP user, there is only one SCCP. It is therefore the responsibility of the SCCP to take all the necessary measures to select the correct message types to be sent out and to segment messages if necessary. To this end, SCCP needs to know whether SAAL capabilities are guaranteed to be available towards the destination. However, since SCCP routing has only limited knowledge of the routing capabilities of the network, it is not always capable of determining the availability of SAAL facilities end-to-end to the final destination. SCCP can at best know this for the path up to the next relay node or gateway. Hence, at certain interworking nodes, a capability needs to be provided that allows conversion of the new message types (LUDT, LUDTS) to the ones supported by narrowband SCCP, and segmenting a long LUDT message into multiple XUDT messages (or possibly multiple LUDT messages if the destination understands them), or truncating a long LUDTS to fit into a single XUDTS message, if necessary.

Several possible interworking scenarios are considered:

1. Interworking at the MTP level;
2. Interworking at the SCCP level; and
3. Interworking at the application level.

NOTE - In Figure 9, $SCCP_1$ refers to a version of SCCP compliant with T1.112-1996 (but not necessarily including the extensions for long message capabilities), and $SCCP_2$ refers to a version of SCCP compliant with T1.112-1996, including the extensions for the use of long message capabilities. These versions continue to cover all of the functionality provided in the past. In case 1, the term 'new MTP level 3' covers a MTP-3 able to manage interworking in a mixed MTP network having a mixture of narrowband and SAAL links.

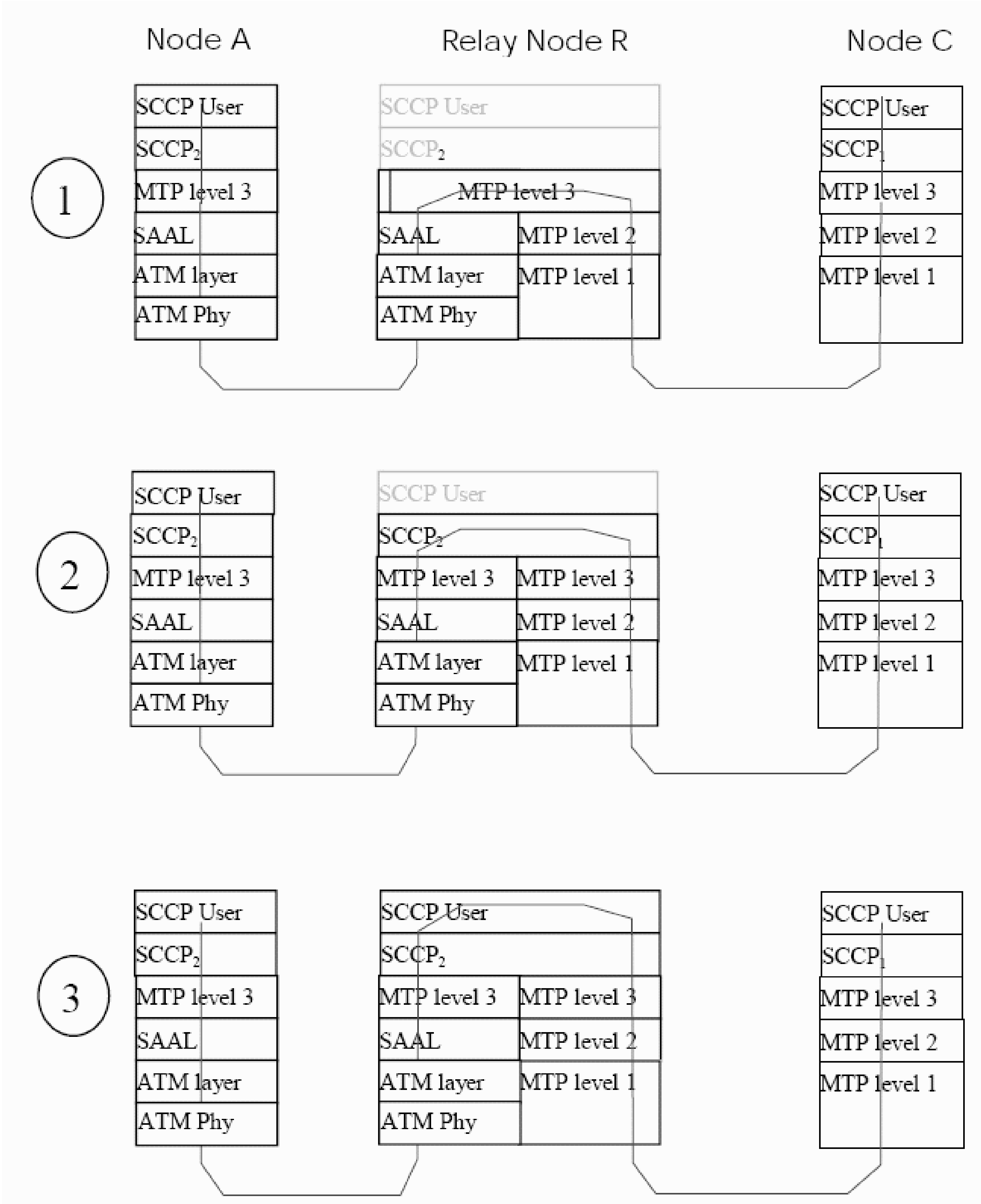


Figure 13 - Protocol stacks for different interworking scenarios

4.5.2.1 Interworking at the MTP level

In mixed networks having a mixture of narrowband and SAAL links, interworking could occur at the MTP level. A message initially sent out over a SAAL link may be transferred to a MTP level 2 (ATIS-1000111.3) link. The SCCP is unaware of such transitions. Only through administrative measures can it be ensured that the SCCP at node A considers node C not reachable with messages that are longer than can be carried by MTP level 2.

4.5.2.2 Interworking at the SCCP level

Since the SCCP is not always aware of the attributes of the complete route towards the destination, interworking nodes are provided where a conversion can be made from the enhanced capabilities to the previously existing ones. The tasks carried out by this interworking node may be:

- Conversion of LUDT messages to XUDT messages; or
- Segmenting long (i.e., the user data of which doesn't fit into one XUDT message) LUDT messages to multiple XUDT messages.

Optionally, the interworking function might also provide the conversion of a XUDT(S) in a LUDT(S) message -- but only when no segmenting of the XUDT(S) is needed due to the length increase of the LUDT(S).

4.5.2.3 Interworking at the application level

Interworking may also be provided by the application itself. However, the SCCP is able to handle all aspects of interworking that are due to the different MTP environments itself. An application interworking function therefore only makes sense if the application has to perform some specific application interworking tasks when going from a broadband network to a narrowband one or vice versa.

4.5.2.4 Further Interworking cases

In practice, combinations of the various situations described will be encountered, especially in the initial stages of introduction of B-ISDN services.