



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.715

(04/2002)

SERIES Q: SWITCHING AND SIGNALLING

Specifications of Signalling System No. 7 – Signalling
connection control part (SCCP)

Signalling connection control part user guide

ITU-T Recommendation Q.715

ITU-T Q-SERIES RECOMMENDATIONS
SWITCHING AND SIGNALLING

| | |
|--|--------------------|
| SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE | Q.1–Q.3 |
| INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING | Q.4–Q.59 |
| FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN | Q.60–Q.99 |
| CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS | Q.100–Q.119 |
| SPECIFICATIONS OF SIGNALLING SYSTEM No. 4 | Q.120–Q.139 |
| SPECIFICATIONS OF SIGNALLING SYSTEM No. 5 | Q.140–Q.199 |
| SPECIFICATIONS OF SIGNALLING SYSTEM No. 6 | Q.250–Q.309 |
| SPECIFICATIONS OF SIGNALLING SYSTEM R1 | Q.310–Q.399 |
| SPECIFICATIONS OF SIGNALLING SYSTEM R2 | Q.400–Q.499 |
| DIGITAL EXCHANGES | Q.500–Q.599 |
| INTERWORKING OF SIGNALLING SYSTEMS | Q.600–Q.699 |
| SPECIFICATIONS OF SIGNALLING SYSTEM No. 7 | Q.700–Q.799 |
| General | Q.700 |
| Message transfer part (MTP) | Q.701–Q.709 |
| Signalling connection control part (SCCP) | Q.711–Q.719 |
| Telephone user part (TUP) | Q.720–Q.729 |
| ISDN supplementary services | Q.730–Q.739 |
| Data user part | Q.740–Q.749 |
| Signalling System No. 7 management | Q.750–Q.759 |
| ISDN user part | Q.760–Q.769 |
| Transaction capabilities application part | Q.770–Q.779 |
| Test specification | Q.780–Q.799 |
| Q3 INTERFACE | Q.800–Q.849 |
| DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1 | Q.850–Q.999 |
| PUBLIC LAND MOBILE NETWORK | Q.1000–Q.1099 |
| INTERWORKING WITH SATELLITE MOBILE SYSTEMS | Q.1100–Q.1199 |
| INTELLIGENT NETWORK | Q.1200–Q.1699 |
| SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000 | Q.1700–Q.1799 |
| SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC) | Q.1900–Q.1999 |
| BROADBAND ISDN | Q.2000–Q.2999 |

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation Q.715

Signalling connection control part user guide

Summary

This Recommendation gives guidance to Administrations, specifiers of SCCP applications and implementors on a number of specific issues related to the incorporation of SCCP in actual networks. These guidelines aim to provide a common understanding and hence to enhance the interoperability between networks and implementations. The aim is to give guidance only, it is not intended to extend, change, nor restrict the normative clauses in ITU-T Recs. Q.711 to Q.714. The following topics are covered in this Recommendation:

- **Compatibility issues:** This Recommendation identifies changes between the different revisions of the SCCP Recommendations and discusses the effect on the interaction between implementations according to the different revisions. Where incompatibilities are unavoidable, engineering measures and evolution strategies are considered.
- **Addressing issues:** The meaning of the different addressing parameters and options is explained. A procedure is provided so that an application specifier can derive the needs and requirements on the addressing in the underlying SCCP layer.
- **Networking issues:** The possibilities of SCCP routing and management are explored to create particular network structures. Also networking issues pertaining to connectionless or connection oriented services are discussed. **Architecture and interworking issues related to broadband SCCP enhancements are also covered.**

Source

ITU-T Recommendation Q.715 was revised by ITU-T Study Group 11 (2001-2004) and approved under the WTSA Resolution 1 procedure on 13 April 2002.

Keywords

Addressing, congestion, routing, SCCP, Signalling System No. 7, user guide.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

© ITU 2002

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

| | Page |
|-------|--|
| 1 | Scope 1 |
| 2 | References..... 1 |
| 3 | Definitions 2 |
| 3.1 | Terms defined by this Recommendation..... 2 |
| 3.2 | Terms defined in other Recommendations..... 3 |
| 4 | Abbreviations..... 4 |
| 5 | Conventions 5 |
| 6 | Compatibility issues 5 |
| 6.1 | Overview of differences between editions 5 |
| 6.1.1 | Differences between <i>Red Book</i> and <i>Blue Book</i> 5 |
| 6.1.2 | Differences between <i>Blue Book</i> and the <i>1993 edition</i> 7 |
| 6.1.3 | Differences between the <i>1993 edition</i> and <i>1996 edition</i> 8 |
| 6.1.4 | Differences between the <i>1996 edition</i> and <i>2001 edition</i> 10 |
| 6.2 | Interworking problems 11 |
| 6.2.1 | <i>Red Book</i> to <i>Blue Book</i> interworking 11 |
| 6.2.2 | <i>Blue Book</i> to <i>1993 edition</i> interworking..... 14 |
| 6.2.3 | <i>1993 edition</i> to <i>1996 edition</i> interworking 16 |
| 6.2.4 | <i>1996 edition</i> to <i>2001 edition</i> interworking 21 |
| 6.3 | Compatibility test and message change procedures 21 |
| 7 | Use of addressing parameters 22 |
| 7.1 | Description of addressing parameters in primitives 22 |
| 7.1.1 | Subsystem numbers (3.4.2.2/Q.713) 23 |
| 7.1.2 | The global title..... 24 |
| 7.1.3 | Use of non-standardized TT and SSN in the international network..... 28 |
| 7.2 | Procedure to derive SCCP-addressing requirements..... 29 |
| 7.3 | Global title conversion operations..... 30 |
| 7.4 | The generic numbering plan 31 |
| 7.4.1 | Example 32 |
| 7.4.2 | Considerations for introduction of the generic numbering plan..... 33 |
| 7.5 | Considerations for the SCCP users on the inputs for global title 33 |
| 8 | SCCP networking aspects..... 33 |
| 8.1 | Network structures in view of SCCP management capabilities..... 33 |
| 8.1.1 | Configurations of subsystems..... 34 |
| 8.1.2 | Unambiguous addresses..... 37 |
| 8.1.3 | Load distribution 38 |

| | Page |
|-------|---|
| 8.1.4 | Configurations of relay/gateway nodes 40 |
| 8.2 | Application of connection-oriented services 40 |
| 8.2.1 | Coupling of connection sections (clause 3/Q.714)..... 40 |
| 8.3 | Application of connectionless services 41 |
| 8.3.1 | The return on error procedure (4.2/Q.714)..... 41 |
| 8.3.2 | Maximal length supported by SCCP connectionless procedures 44 |
| 8.4 | Support of MTP-3b..... 45 |
| 8.4.1 | Protocol architecture..... 45 |
| 8.4.2 | Interworking 47 |
| 9 | SCCP congestion handling 49 |
| 9.1 | Assigning importance values to application messages..... 49 |
| 9.2 | Responsibilities for the application 50 |
| 9.3 | Application of MTP congestion procedures..... 51 |
| 9.4 | Application of SCCP and node congestion procedures..... 51 |
| 9.5 | Coordination of congestion control measures between SCCP and other MTP users..... 51 |
| 10 | SCCP support for Number Portability 52 |

Introduction

This Recommendation gives guidance to Administrations, protocol specifiers and implementors on a number of issues related to the application of the SCCP protocol in actual networks.

Background

The SCCP Recommendations have gone through a number of revisions from the 1984 edition (*Red Book*), 1988 edition (*Blue Book*), 1993 edition, 1996 edition up to this edition (2002). During these revisions, incompatibilities were introduced that require extra attention both for the implementation as for the engineering of the networks. These compatibility issues prior to the 1996 edition were not described in the Recommendations.

During the revisions of the Recommendations, flexibility in the addressing mechanisms was introduced. Unfortunately, this flexibility leads to some lack of clarity: it is not clear how these mechanisms can be used in a standardized way to guarantee interworking or future extendibility. This has led to different philosophies being applied in different regions of the world. This user guide does not intend to make any of these historic approaches obsolete, it merely tries to document what is sensible to do and what is not.

SCCP management is another area that is open for interpretation. In this user guide a number of possible network structures and their addressing-requirements are discussed. In practice, not all of these possibilities may be supported by particular implementations.

SCCP congestion was a topic that has long remained for further study. This user guide gives guidelines on how to use the SCCP congestion control measures, specified in the 1996 edition, and further guidelines on how to handle congestion occurring in CCS7 networks.

In order to support B-ISDN services via ATM links, the MTP was upgraded to provide for larger message sizes and higher signalling data rates. The SCCP was enhanced (1996 edition) in order to exploit those new capabilities of the "MTP-3b".

ITU-T Recommendation Q.715

Signalling connection control part user guide

1 Scope

This Recommendation belongs to a set of Recommendations specifying the SCCP protocol (ITU-T Recs. Q.711 [1], Q.712 [2], Q.713 [3], Q.714 [4] and Q.716 [5]). In addition to the protocol aspects in these Recommendations, this additional Recommendation gives guidance to Administrations, specifiers of SCCP-applications and implementors on a number of specific issues related to incorporating SCCP in actual networks. These guidelines aim to provide a common understanding and hence enhance interoperability between network and implementations. Specifically, the following areas are currently included:

- a) Compatibility issues: This Recommendation identifies changes between the several revisions to the SCCP Recommendations, discusses their effect on the cooperation between implementations of different versions and, where incompatibilities are unavoidable, identifies engineering measures and the need for evolutionary strategies to cope with the problems.
- b) Use of addressing parameters: This Recommendation discusses the meaning of the addressing parameters and options that have been introduced over the years. It provides a procedure that an application specifier can apply to derive the needs and requirements on the addressing mechanisms in the underlying SCCP layer.
- c) Network structures: This Recommendation explores the possibilities of SCCP routing and SCCP management procedures to create particular network structures. It discusses the network issues in case of the use of connection oriented services (e.g. coupling of connection sections) and connectionless services (e.g. the return on error procedure).
Interworking issues between (a part of) an MTP network providing the MTP-3b capabilities (Higher SDU-size and data rate, see ITU-T Rec. Q.2210 [16]) and one that does not are described.
- d) Congestion handling: Guidance is given to application specifiers/implementors on how to handle congestion situations reported from the underlying network layers and how to use the capabilities described in SCCP Recommendations.
- e) A brief statement regarding SCCP's ability to support Number Portability.

The aim of this Recommendation is to give guidance only, it is not intended to extend, change nor restrict the normative clauses in Recommendations protocol (ITU-T Recs. Q.711 [1], Q.712 [2], Q.713 [3], Q.714 [4] and Q.716 [5]). In case of conflict, the latter take precedence, e.g. normative aspects of compatibility are described in ITU-T Rec. Q.714.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent editions of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

- [1] ITU-T Recommendation Q.711 (2001), *Functional description of signalling connection control part*.

- [2] ITU-T Recommendation Q.712 (1996), *Definition and function of signalling connection control part messages*.
- [3] ITU-T Recommendation Q.713 (2001), *Signalling connection control part formats and codes*.
- [4] ITU-T Recommendation Q.714 (2001), *Signalling connection control part procedures*.
- [5] ITU-T Recommendation Q.716 (1993), *Signalling System No. 7 – Signalling Connection Control Part (SCCP) performance*.
- [6] ITU-T Recommendation Q.775 (1997), *Guidelines for using transaction capabilities*.
- [7] ITU-T Recommendation Q.1400 (1993), *Architecture framework for the development of signalling and OA&M protocols using OSI concepts*.
- [8] ITU-T Recommendation X.650 (1996), *Information technology – Open Systems Interconnection – Basic Reference Model: Naming and addressing*.
- [9] ITU-T Recommendation X.200 (1994), *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.
- [10] ITU-T Recommendation X.213 (2001), *Information technology – Open Systems Interconnection – Network service definition*.
- [11] ITU-T Recommendation Q.752 (1997), *Monitoring and measurements for Signalling System No. 7 networks*.
- [12] ITU-T Recommendation Q.708 (1999), *Assignment procedures for international signalling point codes*.
- [13] ITU-T Recommendation E.164 (1997), *The international public telecommunication numbering plan*.
- [14] ITU-T Recommendation Q.703 (1996), *Signalling link*.
- [15] ITU-T Recommendation Q.704 (1996), *Signalling network functions and messages*.
- [16] ITU-T Recommendation Q.2210 (1996), *Message transfer part level 3 functions and messages using the services of ITU-T Recommendation Q.2140*.
- [17] ITU-T Recommendation Q.1290 (1998), *Glossary of terms used in the definition of intelligent networks*.

3 Definitions

3.1 Terms defined by this Recommendation

3.1.1 solitary: A node/subsystem is called solitary for a certain portion of traffic, if it is the only node/subsystem capable of handling that traffic.

3.1.2 relay: A node that performs SCCP message transfer without any reference to an application.

3.1.3 replicated: A set of nodes/subsystems is called replicated (e.g. duplicated, triplicated, quadruplicated) for a certain portion of the traffic, if each member of the set is capable of handling that portion of the traffic.

3.1.4 primary: A node/subsystem is said to be the "primary" node/subsystem for a certain portion of traffic, if, in the absence of any failures or administrative blockings, it handles that portion of the traffic.

3.1.5 backup: A node/subsystem is said to be a "backup" node/subsystem for a certain portion of traffic, if, in the presence of failures or administrative blockings that prevents the "primary" from handling the traffic, it assumes the handling of that portion of traffic.

3.1.6 loadsharing: Loadsharing is a mechanism that makes sure that when several nodes/subsystems are capable of handling a certain portion of traffic, each of these nodes/subsystems gets a fair share of that traffic to handle, corresponding to its capacity for handling traffic.

3.1.7 active: A piece of equipment (e.g. a switch) is active when it is performing the functions for which it has been designed.

3.1.8 standby: A piece of equipment is standby when it is in a state where it is able to perform the functions for which it has been designed, but it is currently not used.

3.2 Terms defined in other Recommendations

- a) This Recommendation makes use of the following SCCP terms defined in ITU-T Rec. Q.712 [2]:
 - i) definition of SCCP messages (CR, CC, CREF, DT1, DT2, IT, EA, ED, UDT, RSR, RSC, AK, UDTS, RLSD, RLC, ERR, XU DT, XU DTS, SOG, SOR, SSP, SSA, SST, SSC, LUDT, LUDTS);
 - ii) definition of SCCP parameters.
- b) This Recommendation makes use of the following term defined in ITU-T Rec. Q.1400 [7]:
 - Subsystem number
- c) This Recommendation makes use of the following terms defined in ITU-T Rec. Q.713 [3] and 2.4/Q.714 [4]:
 - Global title indicator
 - Routing indicator
 - Encoding scheme
 - Translation type
 - Numbering plan
 - Odd/even indicator
- d) This Recommendation makes use of the following term defined in ITU-T Rec. X.650 [8]:
 - Unambiguous
- e) This Recommendation makes use of the following terms defined in ITU-T Rec. X.200:
 - Single association control function
 - Application entity
- f) This Recommendation makes use of the following terms defined in ITU-T Rec. Q.1290:
 - Service Switching Point (SSP)
 - Service Control Point (SCP)
 - Service subscriber

4 Abbreviations

This Recommendation uses the following abbreviations.

| | |
|--------|--|
| AC | Authentication Centre |
| AE | Application Entity |
| ASE | Application Service Element |
| ATM | Asynchronous Transfer Mode |
| DPC | Destination Point Code |
| EOP | End of Optional Parameters |
| ES | Encoding Scheme |
| FE | Functional Entity |
| GT | Global Title |
| GTI | Global Title Indicator |
| HLR | Home Location Register |
| IMSI | International Mobile Subscriber Identity |
| IN | Intelligent Network |
| ISDN | Integrated Services Digital Network |
| ISUP | ISDN User Part |
| ITCC | International Telecommunication Charge Card |
| LU DT | Long Unitdata Message |
| LU DTS | Long Unitdata Service Message |
| MAP | Mobile Application Part |
| MSC | Mobile Switching Centre |
| MTP-3b | Message Transfer Part, level 3 with broadband enhancements |
| NAI | Nature of Address Indicator |
| NP | Numbering Plan |
| NSDU | Network Service Data Unit |
| OMAP | Operation, Maintenance and Administration Part |
| OPC | Originating Point Code |
| OSI | Open System Interconnection |
| RI | Routing Indicator |
| RSC | Reset Confirm |
| RSC | Restart Confirm |
| RSR | Reset Request |
| RSR | Restart Request |
| SAAL | Signalling ATM Adaptation Layer |
| SACF | Single Association Control Function |
| SAP | Service Access Point |

| | |
|------|---|
| SCCP | Signalling Connection Control Part |
| SCMG | SCCP Management |
| SCP | Service Control Point |
| SDL | Specification and Description Language |
| SIB | Service Independent Building Block |
| SPC | Signalling Point Code |
| SSC | SCCP/Subsystem Congested |
| SSN | SubSystem Number |
| SSP | Service Switching Point |
| TC | Transaction Capabilities |
| TCAP | Transaction Capabilities Application Part |
| T-fr | Freeze Timer |
| TMN | Telecommunication Management Network |
| TT | Translation Type |
| VLR | Visitor Location Register |

5 Conventions

This Recommendation was drafted according to the guidelines in ITU-T Rec. A.1500 (Appendix I/A.3).

6 Compatibility issues

Several changes were made to the SCCP Recommendations during the study period leading to the 2001 edition. The purpose of this clause is to record these changes, to mention any interworking problems that might arise and to suggest possible solutions to any such interworking problems. For completeness, the changes made during the study periods leading to the previous editions are also covered.

6.1 Overview of differences between editions

6.1.1 Differences between *Red Book* and *Blue Book*

6.1.1.1 Protocol class 4

Protocol class 4 was deleted, there having been no proposals for the procedures to differentiate it from protocol class 3. Therefore protocol class 4 can only have been implemented in either a network or implementation-specific way.

6.1.1.2 RSR and RSC messages

Two message types were deleted, the restart request and the restart confirm. The *Red Book* did not define their use, thus they can only be implemented in either a network or implementation specific way, although a *Red Book* node would not report them to SCCP management as undefined.

6.1.1.3 SSA, SSP, SST, SOR and SOG messages and management procedures

A functional block was added containing SCCP management procedures, and five message types were defined for SCCP management: subsystem allowed, subsystem prohibited, subsystem status test, subsystem out-of-service request and subsystem out-of-service grant.

6.1.1.4 SSC message

The subsystem congested message type, suggested for SCCP management was deleted. The *Red Book* did not define its use, thus it can only be specified in either a network or implementation specific way.

6.1.1.5 Diagnostic parameter

The diagnostic parameter was re-named as "return cause" for the connectionless protocol classes and was deleted from the connection oriented protocol classes.

6.1.1.6 Global title formats and global title indicator parameters

Three new global title formats were defined: GT-type 2, GT-type 3 and GT-type 4. In addition, the "GT-included" field was extended from one bit to four bits and re-named to "global title indicator" field to distinguish the different types of GT formats.

6.1.1.7 Routing indicator

A spare field in the address indicator field was defined as the routing indicator.

6.1.1.8 Translation type, encoding scheme and numbering plan indicator

These three new parameters were added. Their inclusion in an address depends on the GT-format type. The GT-type 1 introduced in the 1984 edition (*Red Book*) consisted only of the nature of the address field.

6.1.1.9 Release causes

Many release causes were re-named and new causes were allocated. The "unqualified" cause was reassigned from "0000 1001" to "0000 1111".

6.1.1.10 Reset causes, error causes and refusal causes

Reset, error and refusal causes were assigned for the first time.

6.1.1.11 Inactivity test

Some mandatory parameters were added to the inactivity test message and used to check for consistency of the connection data.

6.1.1.12 Restart procedure and T-guard timer

The restart procedure was defined for the connection oriented protocol classes. The restart procedure incorporates a new timer T-guard.

6.1.1.13 T-fr freeze timer

The timer for frozen connection references was replaced by an implementation-dependent mechanism.

6.1.1.14 Annex A/Q.713

Annex A was added to ITU-T Rec. Q.713, showing how the release, reset and error causes should be mapped onto the X.213 primitives.

6.1.1.15 SDLs corrected

The SDLs were changed to make them match the text of ITU-T Recs. Q.711 and Q.714.

6.1.2 Differences between *Blue Book* and the 1993 edition

6.1.2.1 XUDT and XUDTS messages

Two new messages were defined, known as "extended unitdata (XUDT)" and "extended unitdata service (XUDTS)". See 1.22/Q.712 and 1.23/Q.712. These two new message types carry two new parameter types, known as "hop counter" and "segmentation"; see 6.1.2.2, 6.1.2.3.

6.1.2.2 Hop counter

A new parameter was defined, known as the "hop counter", see 2.19/Q.712.

6.1.2.3 Segmentation

A new parameter was defined, known as "segmentation", see 2.20/Q.712. Procedures were specified for the segmenting and reassembly of connectionless protocol class messages, see 4.1.1/Q.714. Additional code points were assigned for return causes representing errors encountered during the reassembly process.

6.1.2.4 Timer values

A specific range of values was assigned to each of the timers defined in C.4/Q.714.

6.1.2.5 Subsystem number allocation

Subsystem numbers have been allocated to new applications. For example, Mobile Service Switching Centre (MSC), Visitor Location Register (VLR), see 3.4.2.2/Q.713.

6.1.2.6 Quality of service parameter

The quality of service parameter was clarified to be a "provider option" in the N-UNITDATA indication primitive and as a "user-option" in the N-UNITDATA request primitive. See 2.2.2.3.1/Q.711.

6.1.2.7 Connection oriented abnormal release procedures

Some modifications were made to the connection oriented procedures concerning release due to abnormal circumstances (e.g. routing failure).

6.1.2.8 Sequence control at relay nodes

The requirement to maintain the sequence of protocol class 1 messages with the same sequence control parameter value was made explicit. This is especially important for relay-nodes.

6.1.2.9 Guidelines for addressing

A set of guidelines was agreed for the use of the address information elements in the international network. See Annex E/Q.714, 1993 edition.

6.1.2.10 Routing procedures

The routing procedures were clarified and presented in a revised way to cover all possibilities, see 2.3/Q.714.

6.1.2.11 Restart procedures

Procedures were specified to cover SCCP restart and the SCCP handling of local MTP availability at the end of MTP-Restart, see 5.2.5/Q.714 and 5.4/Q.714. This includes the broadcast of "subsystem allowed" messages referring to SSN = 1 to all "concerned" nodes, see 5.3.7.3/Q.714.

6.1.2.12 Signalling node status management

The procedures for handling the MTP-RESUME indication primitive were modified which also incorporated the handling of an unavailable remote SCCP becoming available again.

6.1.2.13 Accessibility test of remote SCCP

The use of Subsystem Status Test (SST) and Subsystem Allowed (SSA) messages was extended to enable them to refer to SSN = 1, corresponding to the complete SCCP function at a node. See 5.3.4.2/Q.714 and 5.3.4.3/Q.714.

6.1.2.14 Release procedures

The release procedures were clarified. A new repeat-release timer was introduced. The "interval timer" is now only started after the time-out of the release timer, the repeat-release timer then takes over the process of repeating the RLSD message. This procedure is different from that indicated in the *Blue Book* SDLs.

6.1.2.15 SDL corrections

Some SDL corrections were undertaken.

6.1.3 Differences between the 1993 edition and 1996 edition

6.1.3.1 Message formatting

In the message formats, the possibility of leaving gaps between parameters was excluded. This was not explicitly stated in the past, so that implementations may exist that actually have gaps in messages.

The possibility that the block of optional parameters occurs before or between the mandatory variable parameters was explicitly stated, whereas this was not apparent from earlier versions of SCCP Recommendations.

6.1.3.2 Deletion of replacement mode

The replacement mode was left for further study in previous editions of the Recommendations. Since no user for the replacement was identified, it was deleted.

6.1.3.3 Introduction of congestion handling procedures

A new congestion handling procedure was introduced. This caused:

- changes to the N-CONNECT, N-DATA, N-DISCONNECT, N-UNITDATA req. and N-NOTICE primitives to introduce the importance parameter;
- changes to the N-PCSTATE ind. primitive to introduce the restricted importance level;
- the reinstatement of the SCCP management message SSC (removed from *Blue Book*, see 6.1.1.4);
- additional checks in the SCCP routing control.

6.1.3.4 Explicit inclusion of message compatibility rules

The application of the compatibility rules in ITU-T Rec. Q.1400 [7] to the particular case of SCCP were now explicitly covered in ITU-T Rec. Q.714.

6.1.3.5 Values of inactivity timers

The values of the inactivity send, inactivity receive and guard timers, left as provisional values in the *1993 edition*, were specified.

6.1.3.6 Inactivity control procedure

The inactivity control procedure was made mandatory on all connection sections. The "option" to leave connection supervision to the SCCP-user itself was found not to be feasible.

6.1.3.7 Calling party address treatment

The treatment of the calling party address in relay nodes (with and without coupling) was clarified. As a result, the option to have no coupling of connection sections in a relay node is no longer marked for further study.

Modifications of calling party addresses were now allowed.

6.1.3.8 Screening

Screening of calling party addresses was introduced as an optional procedure. The aim being to prevent illegal messages from entering a network through a gateway.

6.1.3.9 Loadsharing

The text describing the different modes of operation of SCCP management was clarified. It now explicitly identifies methods of loadsharing over SCCP nodes (based on the SLS value in case of protocol class 1).

6.1.3.10 Routing failures

The description of routing failures was clarified. The "hop counter violation" was added as an extra routing failure. Further, the refusal causes were brought in line with the return causes, by the addition of several new refusal causes. The refusal, release and return cause "not-obtainable" was deleted.

6.1.3.11 Assignment of TT values

TT values (different from zero), applicable to the international interface, were for the first time standardized.

These values were standardized for use with GTI = 4 (see Annex B/Q.713). The same values may have a different meaning if used with another GTI.

6.1.3.12 New values for NP, TT, SSN

A number of new values for NP (private numbering plan, ITU-T Rec. E.118; generic numbering plan), TT (ISDN end-to-end supplementary services, ITCC), and SSN (ISDN-supplementary services, broadband ISDN edge-to-edge services and the TC-test responder) have standardized. The use of the different combinations of NP, TT and SSN was described in a new Annex B/Q.713 (also replacing Annex E/Q.714, *1993 edition*).

6.1.3.13 New generic numbering plan

A "generic numbering plan" was introduced to unambiguously identify a SCCP node or user entity.

6.1.3.14 Changes to the SDLs

The SDLs were aligned with the texts of the *1993 edition* and extended with new procedures for congestion control and support of broadband signalling.

6.1.3.15 Deletion of receipt confirmation service

The receipt confirmation service, which was always left for further study, was deleted. This caused the deletion of the receipt confirmation service selection parameter, N-DATA ACKNOWLEDGE primitive and confirmation request parameter.

6.1.3.16 Handling of ERR messages

The handling of the ERR message in states other than the data transfer state of a connection is specified in Tables B.2/Q.714 and B.3/Q.714.

6.1.3.17 Clarification of address formats

It was agreed that:

- a) Bit 8 of the address indicator must always be set to 0 in the international network.
- b) In octet 3 of the address format for GTI = 4, bit 8 will always be set to 0.

6.1.3.18 Omission of subsystem multiplicity indicator

The subsystem multiplicity indicator in the subsystem management messages was marked as a national option. Within the international network, it shall always be set to zero.

6.1.3.19 Support of MTP-3b capabilities

To support signalling for B-ISDN, an extension of the MTP level 3 (called "MTP-3b", see ITU-T Rec. Q.2210 [16]) has been defined that allows the transportation of higher capacity signalling messages via SAAL links, with potentially higher data rates than MTP level 2 according to ITU-T Rec. Q.703. To exploit these new capabilities of MTP-3b within SCCP, two new message types were defined (LUDT and LUDTS) that allow the transportation of up to 3968 octets of user data without invoking the segmentation procedures.

6.1.3.20 Removal of maintenance information

All instances, where in previous version "maintenance information" was issued, were removed. In the SDLs they were replaced by "inform OMAP". All these instances are now handled by first and interval measurements defined in ITU-T Rec. Q.752.

6.1.3.21 Message changes

Changes between different message types (for LUDT, LUDTS, XUDDT, XUDDTS, UDT, UDTS) were allowed (see 4.1.2/Q.714). Such changes may be needed:

- if a network supporting broadband SCCP additions is interworked with a network not supporting them;
- to allow a priority level carried in the SIO (national option for congestion control) to be transported in the importance parameter;
- if a network operator has some interest in adding certain parameters (e.g. hop counter).

In some cases, parameters may be added without message type changes.

6.1.3.22 Model of the global title translation process

A model for the global title translation process was introduced in ITU-T Rec. Q.714.

6.1.4 Differences between the 1996 edition and 2001 edition

6.1.4.1 New translator selectors

Translator selectors (TT, NP and NAI combination) with their corresponding address format for international roaming were specified in Annex B/Q.713.

6.1.4.2 Additional application for existing translator selectors

INAP is added as application which might use the address formats B.4.3/Q.713 and B.4.4/Q.713 in both calling – and called party address.

6.1.4.3 MTP/SCCP restart

Clarifications for MTP/SCCP restart are made (5.2.5, 5.2.6 and 5.4/Q.714).

6.1.4.4 Non-standardized SSN transport in the international network

Code points for SSNs which are bilaterally agreed between the end SCCP user entities are allowed to be transported in the international network (Annex B/Q.713 and 2.7.2/Q.714).

6.1.4.5 Additional message change

An additional, optional, message change is added to 4.1.2/Q.714 : UDT(S)↔LUDT(S).

6.1.4.6 OSI alignment

Opportunity was taken to align some of the text in ITU-T Recs. Q.711 and Q.714 with OSI terminology.

6.1.4.7 IT procedures

An ERR message must be sent in reply to a received IT message with unassigned destination local reference.

6.1.4.8 SCCP parameter values

Some of the SCCP parameter value ranges were agreed to be "reserved for national use", with the highest value marked as "reserved" instead of "spare".

These parameters are:

- NAI;
- Release cause;
- Reset cause;
- Error cause;
- Refusal cause.

6.1.4.9 SCCP GT translation function

Text in 2.1, item 1)/Q.714 is changed, the possibility to access an external database during GT translation has been clarified.

6.2 Interworking problems

A number of changes have been introduced into the SCCP Recommendations throughout the different study periods. The major changes have been identified in 6.1 above. Although in many cases there will be no interworking problems, some instances have been identified where problems will arise. This subclause gives guidance on the appropriate action that should be taken in the SCCP to overcome such interworking problems.

6.2.1 Red Book to Blue Book interworking

There were fifteen areas where changes from the *Red Book* to the *Blue Book* might have introduced interworking problems:

- i) Protocol class 4 was deleted;
- ii) the restart request and the restart confirm message types were deleted;
- iii) the five message types for SCCP management were defined and SCCP management procedures introduced;
- iv) the subsystem congested message was deleted;
- v) the diagnostic parameter was renamed as "return cause" for the connectionless protocol classes and was no longer applicable to the connection-oriented protocol classes;
- vi) three new GT formats were specified: GT-type 2, GT-type 3 and GT-type 4 and the "GT Indicator" field was changed;

- vii) a spare field in the address indicator field was defined as the "routing indicator";
- viii) three new parameters were available, depending on the GT format type;
- ix) release cause values were renamed and new values were allocated. The value of the "unqualified" release cause was reassigned;
- x) reset, error and refusal causes were introduced;
- xi) mandatory parameters were added to the inactivity test message;
- xii) the restart procedure for the connection oriented protocol classes was defined, using a new timer "T-guard";
- xiii) T-fr Freeze timer;
- xiv) Annex A/Q.713;
- xv) SDLs corrected.

6.2.1.1 Protocol class 4

Any interworking solutions must be network or implementation specific because protocol class 4 can only be implemented in either a network or implementation specific way.

6.2.1.2 Restart request and restart confirm messages

Any interworking solutions must be network or implementation specific because protocol class 4 can only be implemented in either a network or implementation specific way.

6.2.1.3 SCCP management messages and management procedures

Red Book nodes should not carry backup subsystems for *Blue Book* nodes if coordinated state change is used, because "subsystem out of service request" messages are discarded by *Red Book* nodes.

Blue Book nodes must assume that subsystems, including SCCP management, at *Red Book* nodes are permanently available, because "subsystem status test" messages will be discarded by *Red Book* nodes and "subsystem available" messages will never be sent by *Red Book* nodes.

Red Book nodes should not be marked as "concerned" at *Blue Book* nodes, because *Red Book* nodes will not react to "subsystem prohibited" messages.

6.2.1.4 Subsystem congested message

Any interworking solutions must be network or implementation specific because this message type can only be implemented in either a network or implementation specific way.

6.2.1.5 Diagnostic parameter

The "diagnostic" parameter may be sent by a *Red Book* node in "Released", "Reset" and "error" messages. *Blue Book* nodes should ignore the parameter (ideally the "diagnostic" parameter should have been retained in the *Blue Book* as optional, but ignored). It should be noted that the ERR and RSR messages still contain a pointer to optional parameters, although a node will never receive any optional parameter from post-*Red Book* nodes.

For the connectionless services, a *Red Book* node should map the *Blue Book* values onto a suitable "reason for return" (perhaps "unknown") in an N-NOTICE indication primitive.

6.2.1.6 New GT-formats and global title indicator field

A *Blue Book* node's signalling routing data should be configured to use only GT-type 1 on signalling associations where the next node is implemented to *Red Book* (either a relay node or destination). This is because *Red Book* nodes interpret addresses with GT-types 2 and 4 as containing no global title. Additionally addresses with GT-type 3 are recognized as GT-type 1, causing syntax failures.

6.2.1.7 Routing indicator parameter

The signalling routing data of a *Blue Book* node that follows a *Red Book* node should include GT translation data for the cases where the *Red Book* node's signalling routing data yields addresses comprising GT+DPC+SSN. This is because a *Red Book* node always sets the routing indicator field to "0", meaning "route on GT".

In the case of an address comprising of GT+DPC+SSN, it is implementation dependent which of them will be chosen for routing, because a *Red Book* node ignores the routing indicator. This should be considered when constructing the signalling routing data of a *Blue Book* node that precedes a *Red Book* node.

6.2.1.8 New address parameters

The solution in 6.2.1.6 means that the new address parameters are not used towards *Red Book* nodes, thus avoiding the interworking problem that would otherwise exist.

6.2.1.9 New and renamed "release cause" values

If a *Red Book* node uses the "unqualified" value of the "release cause", it is incorrectly interpreted by a *Blue Book* node as meaning "subsystem congested", however the protocol is not affected (ideally, the *Blue Book* should not have re-assigned the value for "unqualified").

6.2.1.10 Reset, error and refusal causes

A *Red Book* node will always use the value "0000 0000", causing incorrect interpretation at a *Blue Book* node, however the protocol is not affected (ideally, the *Blue Book* should have assigned the value "0000 0000" as "unqualified").

A *Red Book* node should map the *Blue Book* values onto a suitable "reset reason" or "disconnect reason" (perhaps "unknown") in an N-RESET or N-DISCONNECT indication primitive as appropriate.

6.2.1.11 Parameters added to the inactivity test message

The *Blue Book* nodes should be modified to treat the missing parameters as optional or the procedure should be suppressed on signalling associations between *Red Book* nodes and *Blue Book* nodes (ideally, the extra parameters in the *Blue Book* should have been optional).

6.2.1.12 Restart procedure for the connection oriented protocol

Any interworking solutions must be network or implementation specific, because the restart procedure can only be implemented by a *Red Book* node in either a network or implementation specific way; if the inactivity test procedure cannot be used (see 6.2.1.11), then there is a risk that some of the connection references might become "locked up" following a restart at a *Red Book* node.

6.2.1.13 T-fr freeze timer

No extra interworking problems are foreseen because it affects only the internal operation. However, *Blue Book* implementations should allow adequate "frozen" time, when interworking with *Red Book* nodes and other *Blue Book* nodes.

6.2.1.14 Annex A/Q.713

No protocol interworking problems are foreseen between signalling points because the change only affects the internal interface of a node.

6.2.1.15 SDLs corrected

No interworking problems are foreseen.

6.2.2 *Blue Book* to 1993 edition interworking

There were fifteen areas where changes from the *Blue Book* to the 1993 edition might have introduced interworking problems:

- i) XUDT and XUDTS message types;
- ii) hop counter;
- iii) segmenting and reassembly procedures;
- iv) timer values;
- v) subsystem number allocation;
- vi) quality of service parameter;
- vii) connection oriented abnormal release procedures;
- viii) sequence control at relay nodes;
- ix) guidelines for addressing;
- x) routing procedures;
- xi) restart procedures;
- xii) remote SCCP status management procedures;
- xiii) test for the accessibility of a remote SCCP;
- xiv) change in release procedures;
- xv) SDL corrections.

The suggested action required at the *Blue Book* and/or 1993 edition node to enable interworking is contained in the following items.

6.2.2.1 XUDT and XUDTS message types

A *Blue Book* node will discard XUDT and XUDTS message types, if received.

One possible approach is to upgrade *Blue Book* relay nodes such that they treat the XUDT and XUDTS message types as UDT and UDTS types respectively, with the possible addition of handling the hop counter parameter, see 6.2.2.2.

6.2.2.2 Hop counter

No interworking problems are foreseen due to the hop counter parameter itself. If it is in the CR message, it would be carried transparently by nodes using a version of SCCP older than the 1993 edition. If it is in the XUDT or XUDTS messages, the messages would be discarded as "unknown message type" by any node using a version of SCCP older than the 1993 edition.

6.2.2.3 Segmenting and reassembly procedures

The signalling routing data of a 1993 edition node should be configured such that applications requiring the segmenting/reassembly service are not assigned a signalling association involving *Blue Book* nodes either as relay nodes or as destination node. However, the only additional requirement on the relay nodes is the ability to transfer the XUDT and XUDTS message types, see 6.2.2.1 and 4.18/Q.713 and 4.19/Q.713.

Since XUDT/XUDTS messages are simply discarded by *Blue* or *Red Book* nodes, there is no possibility of reverting to using UDT/UDTS when transport of the message is not successful. This incompatibility caused by the XUDT and XUDTS messages necessitates that these message types and the related segmenting/reassembly procedures are introduced in a carefully planned way:

- Before any application can employ segmenting, it must be assured that all relay nodes and gateways that may be passed are converted to the 1993 edition (or at least have the capability to transfer XUDT/XUDTS messages. The capability for segmenting/reassembly

itself is not required). For international services, multilateral agreements must be reached between Administrations.

- To assure the highest possible chances for interworking, during a transition phase, short messages not needing segmenting/reassembly should be sent using UDT/UDTS.
- After the transition phase, XUDT/XUDTS can be fully introduced, allowing advantage to be taken of the hop counter and other optional parameters.

If an application requiring the segmenting/reassembly service is to be deployed at a *Blue Book* node, the node must, as a minimum, be upgraded with the segmenting/reassembly function and the ability to handle the XUDT and XUDTS message types.

6.2.2.4 Timer values

Where possible, a SCCP implemented to the *Blue Book* should adopt the timer values specified in the *1993 edition* when interworking with a *1993 edition* SCCP. For timer values see C.4/Q.714 and D.4/Q.714.

It should be noted that the inactivity timers (and hence also the guard timer) were left provisional. When nodes with different sets of timer values inter-communicate, it should be guaranteed that the lowest value of T_{ias} in the remote nodes is shorter than T_{iar} in the local node and that the shortest T_{iar} in the remote nodes is still longer than T_{ias} in the local node. See 6.2.3.5 for further information.

6.2.2.5 Subsystem number allocation

No interworking problems are foreseen. If any traffic is inadvertently routed to end or final GT translation nodes with unequipped SSNs, an (X)UDTS message will be generated if the return option is set.

6.2.2.6 Quality of service parameter

No interworking problems are foreseen.

6.2.2.7 Connection oriented abnormal release procedures

No interworking problems are foreseen because only the internal operation of a node is affected.

6.2.2.8 Sequence control at relay nodes

No interworking problems are foreseen because the *Blue Book* does not specify any actions to handle possible mis-sequencing.

6.2.2.9 Guidelines for addressing

No interworking problems are foreseen because only information elements and procedures are used that were already present in the earlier versions of the Recommendations.

6.2.2.10 Routing procedures

No interworking problems are foreseen because all *Blue Book* procedures have been maintained.

6.2.2.11 Restart procedures

No interworking problems are foreseen for the approach of marking remote subsystems (except a selected list) as "allowed", because *Blue Book* nodes will respond with "subsystem Prohibited" to messages routed to unavailable subsystems.

The restart procedure culminates in the broadcast of "subsystem allowed" with SSN = 1 to "concerned" signalling points. *Blue Book* nodes, on receipt of such a message, should ignore it. Also, when possible, *Blue Book* nodes should not be marked as "concerned" at *1993 edition* nodes.

6.2.2.12 Remote SCCP status management procedures

As with the SCCP restart procedure (see 6.2.2.11), no interworking problems are foreseen with marking remote subsystems (except an optional selected list, see item 5) 5.2.3/Q.714) as "allowed".

When a remote SCCP becomes "inaccessible", a test is invoked in order to detect its recovery, see 6.2.2.13.

6.2.2.13 Test for the accessibility of a remote SCCP

The accessibility test involves periodically sending "subsystem status test" messages referring to SSN = 1. A *Blue Book* node, on receipt of such a message, should ignore it, because when the relevant T-Stat.info timer expires at the *1993 edition* node, it assumes that the remote (*Blue Book*) SCCP has recovered.

If the wait for T-Stat.info to expire at the *1993 edition* node results in an unacceptable delay in detecting recovery of the SCCP at a *Blue Book* node, then the *Blue Book* node should be enhanced such that it generates a "subsystem allowed" message in response to "subsystem status test" messages referring to SSN = 1.

6.2.2.14 Change in release procedure

The *1993 edition* describes the release procedure more accurately. To this end, a new repeat-release timer was introduced. The procedure described is however different from the SDLs. Interworking problems are not expected, the only effect may be that a *1993 edition* node repeats the RLSD message one extra time, because the "interval timer" is only started after the first repetition.

6.2.2.15 SDL corrections

No interworking problems are foreseen.

6.2.3 1993 edition to 1996 edition interworking

There were twenty-two areas where changes from the *1993 edition* to the *1996 edition* might have introduced interworking problems:

- i) changes in message formatting;
- ii) deletion of replacement mode;
- iii) congestion handling procedures;
- iv) inclusion of compatibility rules;
- v) values of inactivity timer;
- vi) inactivity control procedure;
- vii) calling party address treatment;
- viii) screening;
- ix) loadsharing;
- x) routing failures;
- xi) assignment of non zero TT values;
- xii) new values for NP and SSN;
- xiii) new generic numbering plan;
- xiv) changes to the SDLs;
- xv) deletion of receipt confirmation;
- xvi) handling of ERR messages;
- xvii) clarification of address formats;
- xviii) omission of subsystem multiplicity indication;

- xix) support of MTP-3b capabilities;
- xx) removal of maintenance information;
- xxi) message changes;
- xxii) global title translation model.

6.2.3.1 Message formatting

Implementations should continue to accept messages that have gaps in them. For the future, messages will be coded at the origin without any gaps. It is preferred that a relay node re-encodes messages received with gaps in order to eliminate the gaps, assuming that this is practical.

Conflicts may occur with older implementations that assume that the optional parameter block is always behind all variable parameters (e.g. by assuming that the end of optional parameters delimits the end of the message). It is therefore advised to put the optional parameter block at the end of the message when interworking with 1993 or older versions of the SCCP.

6.2.3.2 Deletion of replacement mode

This should not cause interworking problems since the option was, as far as is known, not used in practice. Its application would be a purely local matter and not visible on the peer-to-peer protocol.

6.2.3.3 Introduction of congestion handling procedures

No compatibility problems are foreseen:

- If users do not provide an importance value in their primitives, the SCCP will assign a default value (although it is preferable for users to provide the importance value to SCCP).
- Also for all messages received from *1993 edition* (or earlier) nodes, where the importance parameter is not present (and cannot be derived from the priority level in the MTP SIO field, when the national option for MTP congestion is used), a default value will be assigned.
- If a *1993 edition* (or earlier) node receives a message (CR or XU DT) with the optional parameter "importance", this parameter will be passed transparently as required by the compatibility rules of ITU-T Rec. Q.714.
- *1993 edition* (or earlier) nodes will discard the new SCCP management message SSC.

To gain the full advantage of the new congestion control procedures, it is necessary that the UDT messages are gradually replaced by XU DT (or LU DT) messages. See also 6.2.2.2.

6.2.3.4 Inclusion of compatibility rules

The application of the compatibility rules from ITU-T Rec. Q.1400 [7] to the particular case of SCCP are elaborated in ITU-T Rec. Q.714. No compatibility problems are anticipated.

6.2.3.5 Values of inactivity timer

The values of the inactivity send, receive and guard timers, provisional in the *1993 edition*, were fixed. When introducing a change in values to these timers, the constraints on the T_{iar} and T_{ias} ($T_{iar} > T_{ias}$ at other end) must be taken into account. If it is intended to increase the timers, it should first be made sure that the T_{iar} (and T_{guard}) is increased at both sides, before increasing T_{ias} . When decreasing values, T_{ias} is to be decreased first at both ends, prior to decreasing T_{iar} (and T_{guard}).

6.2.3.6 Inactivity control procedure

The inactivity control procedure is now mandatory on all connection sections. The "option" to leave connection supervision to the user (implying end-to-end supervision), was found not to be feasible because of the partitioning of a connection in connection sections.

6.2.3.7 Calling party address treatment

The treatment of the calling party address in relay nodes (with and without coupling) was clarified. As a result, the option to have no coupling of connection sections in a relay node is no longer marked for further study. It can be assumed that a relay node that does not implement the calling party address modification rules (2.7/Q.714) will always act as a relay node WITH coupling of connection sections, so no interworking problems are foreseen. If a node behaves incorrectly however, problems will result with messages going to the wrong nodes and resources left hanging at the originating node. To avoid such problems, it is advisable that the originating node (or node initiating the present connection section) always includes its OPC in the calling party address.

A problem may occur if changes of the calling party address extend the message length. If the message length becomes too long, the message might have to be discarded, because SCCP does not provide a mechanism to segment such messages in relay nodes.

6.2.3.8 Screening

Screening of calling party addresses was introduced as an optional. Its main aim is to prevent messages with an illegal calling party address from entering a national network. Screening is a local procedure and does not modify the SCCP peer-to-peer protocol.

6.2.3.9 Loadsharing

The text of SCCP management describing the different modes of operation of SCCP management is clarified. It now explicitly identifies methods of loadsharing over SCCP-nodes. Its introduction is a purely local matter and not visible in the SCCP peer-to-peer protocol.

6.2.3.10 Routing failures

The description of routing failures was clarified. One new value was introduced (hop counter violation). Several new "refusal causes" have been added, in order to align with the "return causes" provided for routing failures. The refusal/disconnect and reset cause "not obtainable" (previously for further study) was deleted. These changes should not cause incompatibilities, since every implementation must allow forward compatibility for the introduction of new cause-values.

6.2.3.11 Assignment of TT values

1993 (and earlier) editions only specified TT value zero. Therefore, it now may be necessary to upgrade some relay and gateway nodes to support non-zero TT-dependent routing, for all signalling relations on which CCBS, B-ISDN edge-to-edge services or ITCC will be used. Compatibility problems might occur if some implementations would actually ignore the value of the TT and route all traffic in the same way. In this case, portions of traffic can get mis-routed and cause unexpected troubles in parts of a network.

6.2.3.12 New values for NP and SSN

No compatibility problems are foreseen. Any 1993 (or earlier) edition nodes will either return (X)UDTS or reject messages as a result of receiving messages with unsupported NP and/or SSN values. As with unsupported TT values, compatibility problems might occur if some implementations ignore the value of the NP and route all traffic in the same way. In this case, portions of traffic get mis-routed.

6.2.3.13 Generic numbering plan

A new numbering plan, the "generic numbering plan", was introduced to unambiguously identify a SCCP node or user-entity. In this numbering plan, a national identification is encapsulated in a unique number composed of the international SPC (ITU-T Rec. Q.708 (ISPC)) in BCD format, and a national part. The encoding scheme is only applicable to the national part. The international part must "by default" be decoded as BCD. A new value "national specific" is added for the encoding

scheme. In practice, the international part may have to be added to a calling party address and removed from the called party address in the gateways.

Several compatibility issues arise:

- The introduction of a new encoding scheme presents a problem: any node in the network that does not support the encoding scheme will not be able to decode the message it gets, and therefore has to throw away the message as "syntax error": "unknown ES" [see case a4, item 1), 3.8.3.3/Q.714)]. Indeed, any old implementation will interpret the ES as applying only to the complete address information and not just to the national part.
All concerned implementations must therefore be upgraded with the additional logic to recognize the special situation of NP = generic-NP and value of encoding scheme. Only after all the relay nodes and gateways in the networks are upgraded, the new encoding scheme can be introduced. It must be clear that as soon as one country starts using the new encoding scheme in its calling party addresses, all other concerned parties (countries and international carriers) would be forced to accept the new encoding scheme, even though the translation for routing back of the message remains restricted to the international part of the address.
- The application of the new numbering plan necessitates the manipulation of global titles in gateways. These manipulations were defined in the *1993 edition* only for called party addresses (although not fully specified), but not for calling party addresses. Some types of exchanges will first have to be updated to provide these capabilities.

As apparent from these compatibility problems and other considerations mentioned in 7.4.2, the introduction of the new generic numbering plan requires a carefully planned introduction strategy. In a first phase, an alternative solution (like using E.164 numbers) will have to be used for the addressing of ITCC.

6.2.3.14 Changes to the SDLs

The SDLs consolidate the work that has been done in the *1993 edition*. No compatibility problems are introduced.

6.2.3.15 Deletion of receipt confirmation service

The receipt confirmation service, which was always left for further study up to the *1993 edition*, was deleted. This required the deletion of the receipt confirmation selection parameter, N-DATA ACKNOWLEDGE primitive and confirmation request parameter. Since no external protocol elements have been defined to support the option, no compatibility problems can occur.

6.2.3.16 Handling of ERR messages

The handling of the ERR message in states other than the data transfer state of a connection is specified in Tables B.2/Q.714 and B.3/Q.714. The behaviour specified corresponds to what was in the SDLs of the *Blue Book*. Although some implementations might react somewhat differently from others in the error cases, there are no significant incompatibility problems expected, since resources will be released at both sides at the latest when the supervision timings on the different connection phases expire.

6.2.3.17 Clarification of address formats

- a) Bit 8 of the address indicator must always be set to 0 in the international network
Bit 8 can be used to indicate the use of a national specific addressing format (e.g. USA). The address format must however be converted to the internationally valid formats before the message is passed into the international network. Bit 8 must then be set to 0, otherwise the receiving network might start to interpret the address according to its own (different) national format.

- b) In octet 3 of the address format for GTI = 4, bit 8 will always be set to 0

This change was introduced because the same field occurs in the GTI = 1, but for GTI = 1, bit 8 contains the O/E indicator. Any information in this bit would be lost converting from GTI = 4 to GTI = 1 (it is overwritten with the O/E indicator), so it would not be carried transparently as the compatibility rules require it to be a spare field.

6.2.3.18 Omission of subsystem multiplicity indicator

The omission of the subsystem multiplicity indicator does not lead to compatibility problems, since its use was not specified. The SCCP management procedures work without it.

6.2.3.19 Support of MTP-3b capabilities

The introduction of new message types (LUDT, LUDTS) potentially leads to incompatibilities since:

- the new values of the "message type" are not recognized in older versions;
- the formatting rules of the messages differ from the existing SCCP messages (all pointers and the length field of long parameters are extended to two octets);
- the new messages may be longer than 272 octets, in which case they can only be transported if MTP-3b capabilities are available.

On the other hand, it is a requirement that:

- B-ISDN services using SCCP can be also be introduced where only *1993 edition* SCCP is available;
- other existing SCCP users should also be able to benefit from the new capabilities offered by MTP-3b.

Therefore, provisions have been made for:

TRANSPARENCY: The service delivered by SCCP to the SCCP user is not changed. For the SCCP user, whether MTP-3b capabilities are available or not is transparent. SCCP takes all the necessary measures to select the correct message types to be sent out and to segment messages if needed.

INTERWORKING: As SCCP routing control has only limited knowledge of the transport capabilities in the SCCP network, it is not capable of determining the availability of MTP-3b facilities end-to-end to the final destination. SCCP only knows this for the path up to the next relay node or gateway. At certain interworking nodes, capabilities need to be provided that convert the new message types to the types provided by the *1993 edition*, segmenting a long LUDT message into multiple XUDT messages, or truncating a long LUDTS message to fit into one XUDTS message, if necessary.

It is the responsibility of the network operator(s) to ensure through administrative measures that:

- data on the availability of larger message sizes and support of LUDT(S) messages, is consistent with the structure of the underlying MTP network (which may include STPs at which MTP-3b interworks with narrow-band MTP at the MTP level, or contains provisions for backup of MTP-3b routes via narrow-band routes) and the capabilities of the new visited SCCP node;
- interworking nodes with the necessary capabilities are provided at those places where needed.

6.2.3.20 Removal of maintenance information

No interworking problems are foreseen at the protocol level.

6.2.3.21 Message change

It is the responsibility of the network operator to make sure that messages do not enter a part of a network where they are not supported. Care must be taken that the addition of parameters does not exceed the maximum data length supported.

6.2.3.22 Global title translation model

No interworking problems are foreseen, as the model is only a model and does not imply implementation changes.

6.2.4 1996 edition to 2001 edition interworking

No protocol interworking problems are foreseen. Any of the new TT and SSN value assignments received at a 1996 (or earlier) edition node will either be discarded or (L)(X)UDTS sent in response.

6.3 Compatibility test and message change procedures

This clause provides guidance on the possible reasons why the optional message changes listed in 4.1.2/Q.714 could be required. Each message change is appended with one or more possible network interworking scenarios where the change could be necessary.

| From | ⇒ | To | Comment | Possible condition for use |
|-------|---|-------|---|----------------------------|
| LUDT | ⇒ | LUDT | 2-N segments, no message type change but segmentation | (1) |
| XUDT | ⇒ | LUDT | message type change without reassembly | (2) |
| LUDTS | ⇒ | XUDTS | message type change without truncation | (3) |
| XUDTS | ⇒ | LUDTS | message type change without truncation | (2) |
| UDT | ⇒ | XUDT | 2-N segments, message type change with segmentation | (1) or (7) |
| UDT | ⇒ | XUDT | message type change without segmentation | (6) or (7) |
| XUDT | ⇒ | UDT | message type change (note) | (4) |
| UDTS | ⇒ | XUDTS | message type change with possible truncation | (6) |
| XUDTS | ⇒ | UDTS | message type change | (4) |
| UDT | ⇒ | LUDT | message type change | (2) |
| UDTS | ⇒ | LUDTS | message type change | (2) |
| LUDT | ⇒ | UDT | message type change without truncation | (5) |
| LUDTS | ⇒ | UDTS | message type change without truncation | (5) |

NOTE – Only for single XUDT when:

- (1) Maximum message length towards the destination is limited;
- (2) Destination only supports LUDT(S) or use of LUDT(S) is mandatory in the network;
- (3) Destination is *White Book* (1993 or 1996 edition without LUDT(S) support);
- (4) Interworking between 1993 edition SCCP with *Blue Book* SCCP;
- (5) Interworking between 1996 edition SCCP with *Blue Book* SCCP;
- (6) Destination only supports XUDT(S) or use of XUDT(S) is mandatory in the network;
- (7) Request insertion of optional parameter.

7 Use of addressing parameters

SCCP addressing capabilities allow a host of different combinations of parameters for routing. This clause provides some general guidelines on when to make use of the various parameters (such as translation types, subsystem numbers, numbering plans).

7.1 Description of addressing parameters in primitives

SCCP allows two ways for the SCCP user to specify an address: either by addressing an SCCP-SAP by its SPC (+MTP-SAP identification) and SSN (see 7.1.1 for an explanation of SSN), or by global titles.

1) *Using DPC (+MTP-SAP identification) and SSN*

In this case the SSN in the called party address provided by the originating node and delivered to the destination node for selection of the appropriate application entity. The originating SCCP checks the availability and congestion state of the DPC and the SCCP and checks the availability state of the SSN at that DPC before sending out the message to the destination node. No backup or loadsharing facilities can be provided by SCCP when using this type of routing.

2) *Using GT and optionally SSN*

A global title is a sequence of digits or other information elements (called "global title address information", GTAI, see 7.1.2.6), in combination with other information elements such as translation type (see 7.1.2.3), numbering plan (see 7.1.2.1), nature of the address (see 7.1.2.2) that (in possible combination with the SSN), either:

- a) represents an unambiguous¹ identification of an SCCP user-entity in the signalling network. Such identifications can be part of an existing numbering plan, or use a specific "generic" numbering plan devised for this purpose. These unambiguous identifications are normally passed as calling party addresses in SCCP messages to the destination, to allow any return message to be sent back to the correct originating node, by using it as called party address. In TCAP, CONTINUE messages always make use of the unambiguous address sent in the calling party address of the BEGIN or first CONTINUE message to continue with the dialogue; or
- b) is derived from an "access" address to a telecommunications network (e.g. subscriber number, IMSI); or
- c) represents a logical "service address" that allows SCCP to route the message to any SCCP user entity that is capable of providing the requested service.

On the external protocol interface, the "encoding scheme" indicates in which way the digits or other information elements are represented (see 7.1.2.4).

With this type of addressing, routing in the network uses the global title. The subsystem number, if present, does not take part in the digit translation within the network that determines the end-node to be reached (these are the steps 1 and 2 in the routing model of 2.4/Q.714). In relay nodes, the SSN, if present, is normally passed transparently. When the final translation occurs in a relay node, the SSN is used by the addressing and routing function to identify and to determine the state of the subsystem and, where appropriate, to redirect the message to a backup subsystem. The SSN may be provided in the called party address by the originating node. The global title translation process offers the extra flexibility to derive or overwrite an SSN in a relay node (or in the destination node).

¹ Unambiguous is used here as defined in ITU-T Rec. X.650 [8] (OSI reference model for naming and addressing): "A name is unambiguous within a given scope when it identifies one, and only one, object within that scope. Unambiguity does not preclude the existence of synonyms."

7.1.1 Subsystem numbers (3.4.2.2/Q.713)

7.1.1.1 Definition and use

In the context of OSI-addressing, a combination of "network addresses" and "selectors" identifies in the destination node, the higher layer entity. The highest level selector selects the application entity. Extending these principles to SCCP, the subsystem number could be considered to be the highest level selector: so the subsystem number allows the network layer (in an OSI-context: the presentation layer) to select the application entity (i.e. SCCP-subsystem) to which the received NSDU is to be sent.

In accordance with these principles, the notion of a SSN is defined in ITU-T Rec. Q.1400 [7] as follows:

- "Subsystem number (SSN): This identifies a subsystem accessed via the SCCP within a node and may be a "user part" (e.g. ISUP or SCCP management) or an *application entity* containing the TCAP-ASE"; and
- "The point code² and SCCP subsystem number (SSN) are the addressing information that, because of the absence of intervening layers, effectively locate an *AE-type* at a SS No. 7 node."

An application entity is normally composed of a "single association control function" (SACF) that coordinates the cooperation of several "application service elements" (ASE). Further communication can take place between two equivalent peers or asymmetrically between "functional entities" (FE), each having their own role in the system (e.g. SSP/SCP in IN, HLR/VLR in MAP). Within an application, the combination of certain ASEs in FEs can be used to build several different "features" or "services".

The SSN should not be used to provide addressing of individual services, features, functional entities, SIBs or ASEs within an application entity. These items are only roles or subfunctions within a certain application entity. The distribution within an application entity is the task of the SACF function. For TC-based applications ("TC-users"), mechanisms to accomplish this are described in ITU-T Rec. Q.775 [6], the TC-user guide.

The current list of internationally standardized SSNs can be found in 3.4.2.2/Q.713.

Note that the contents of application entities may be implementation dependent.

7.1.1.2 SSN assignment guidelines

New internationally standardized SSNs are allocated by the Working Party within ITU-T, Study Group 11, responsible for SCCP on request of a Working Party responsible for standardizing an international application using SCCP.

New internationally standardized SSNs could be allocated if the subsystem could be reached by SCCP routing in the international network based on PC and SSN. If the subsystem is in the international network and is reached by GT routing in the destination node, standardisation of SSN is ffs.

NOTE 1 – An internationally standardized SSN could be derived in the international network on GT translation.

NOTE 2 – In standardizing an SSN for an SCCP user the need for SCCP management should be examined. If the application wants to make use of SCCP management for functional entities which have to be managed independently, the functional entities have to be different applications entities. Standardization for network management purposes of SSNs is ffs.

² To be entirely accurate, a remote MTP node is identified by both a point code and the identity of the local MTP-SAP.

NOTE 3 – The above criteria are not considered exhaustive. Additional guidelines on assignment of internationally standardized SSNs are for further study.

7.1.2 The global title

7.1.2.1 Numbering plan (NP) (3.4.2.3.2/Q.713)

A numbering plan represents a numbering scheme for users of telecommunication services in different telecommunication networks. For example, E.164 for ISDN allocates numbers for telephony subscribers, E.212 for mobile, etc.

Numbering plans are in general NOT allocated by the ITU-T C7 working parties. They are referred to nevertheless in ISDN-, ISUP-, MAP- and SCCP-messages. The range of numbering plans may in future have to be extended to synchronize with developments outside CCS7.

One specific numbering plan ("generic numbering plan") is defined by SCCP in order to allow nodes or SCCP subsystems in the SS No. 7 network to be numbered unambiguously (see also 8.1.2).

7.1.2.2 Nature of address indication (NAI) (3.4.2.3.1/Q.713)

The NAI identifies the scope (a network, geographical region or other) in which a number is valid (such as the local area, country). This allows shortening the number (and hence the translation process) to the digits that are actually relevant in that particular scope. In the past, nature of the address was represented by "access codes" before the number, for example -00- for international access. The problem with this is that these access codes are country dependent and can therefore not be easily transported in signalling messages across network borders.

The NAI is defined together with a numbering plan. SCCP provides only a coding for the different scopes necessary for SCCP message routing purposes.

7.1.2.3 Translation type (TT) (3.4.2.3.4/Q.713)

In contrast to the previous elements (NP and NAI), the translation type is a pure SCCP concept.

A number, according to a specific NP and NAI, representing an access address may for one value of the translation type be translated such that the node reached by SS No. 7 routing is exactly that node where the access "resides" (i.e. physically connected or administrated). It may nevertheless be necessary to translate the same GTAI for the specific NP and NAI to the address of a service centre instead. In the past this would in some cases have been solved by putting service codes before the number. Such service codes however can be different in every country.

Some information element must therefore be added if it is required to have several translation results for the same GTAI, NP and NAI (e.g. derived from a subscriber number). This information element is the translation type (TT). Different translation types are therefore to be assigned in order to distinguish the different uses of the same NP, NAI and GTAI by different services.

There may be circumstances where routing may have to use information extraneous to the "telephony" world. This is, for example, the case with ITCC, using a charge card number as address. In such a case, there is also a need to define a TT, to avoid the definition of new numbering plans.

7.1.2.3.1 The translation type's role in the GTT function

The function of the final GTT is to translate the global title into an SS No. 7 point code and, especially when not present, a subsystem number type of address (resulting in a DPC, SSN and RI = route on SSN). A complete GT consists of a combination of translation type, NP and/or NAI, and GTAI. Clause 2.1/Q.714 [4] defines a global title as an address, such as dialled-digits, which does not explicitly contain information that would allow routing in the signalling network. There are many classical examples of these addresses: called party dialled digits, the caller's identification

(calling line address) or a billing number. A GT is more than just a set of digits; the digits (address information) could be used and reused by many different services/applications that are provided by the networks. Despite that, the GTT function must correctly translate the GT(+[SSN]) into the appropriate SS No. 7 address [DPC + SSN] represented by the GT. The GTT function is required to make a distinction between different users of the same NP/NAI/GTAI combination.

Clearly, the GTT function must be provided with some additional input that indicates the specific usage of the NP/NAI/GTAI combination. Using the subsystem number (SSN) to indicate the way the digits are to be used by the GTT function is not appropriate, since the SSN is not used by steps 1 and 2 of the GT-translation (see 2.4/Q.714), although it might be an output. Therefore, the "translation type" parameter is introduced to enable the necessary distinction between the different uses of the same NP/NAI/GTAI combination. The translation type parameter appears in all GT-formats except format 1 (provided only for *Red Book* compatibility). The translation type is therefore the key input that differentiates between the use of identical NP/NAI/GTAI combinations.

7.1.2.3.2 Assignment of translation types

There are many factors that should be considered in the assignment of translation types. There is also the question of when services are able to share the same translation type value. It would not be efficient nor feasible to assign every single service a new translation type. A few examples (in the context of IN applications) may help in illustrating the basic considerations needed in order to define the basic rules for the assignment of translation types code values and under what circumstances services can share the same translation type.

Example 1 – A SSP triggers an INAP query to be sent using the calling party number CgPN (NP = E.164, + digits) as the GT – to address Appl. X-Z on different SCPs. See Figure 1.

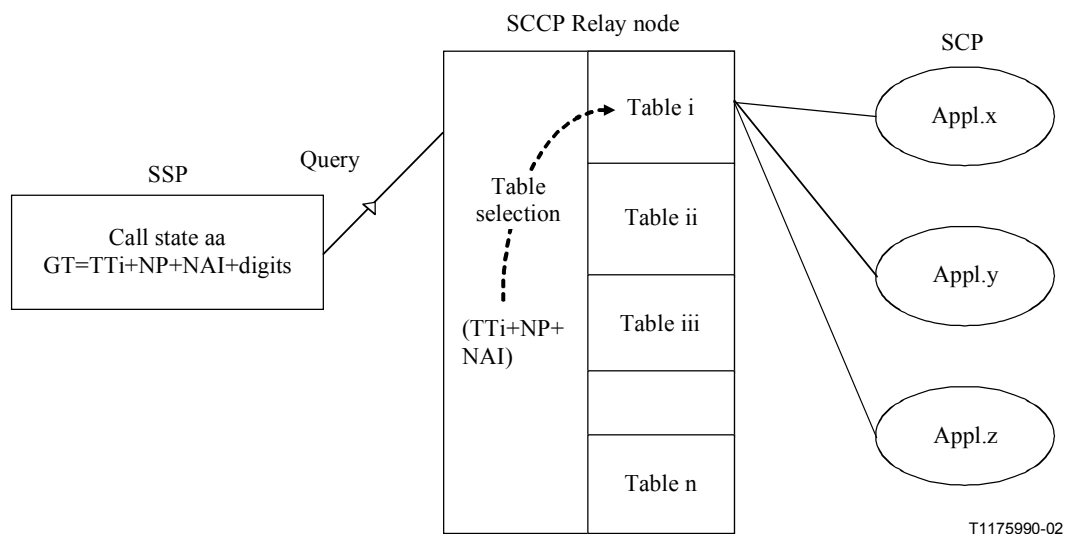


Figure 1/Q.715 – Example 1 of translation type use (CgPN)

Example 2 – A SSP triggers an INAP query to be sent using the called party number (CdPN) as GT. Since the called and calling party number (in Example 1) typically follow the same numbering plan, nature of the address and encoding scheme in a network, different translation types will be required to differentiate Appl. A-C from Appl. X-Z in Figure 1 where use is made of the same GTA I. See Figure 2.

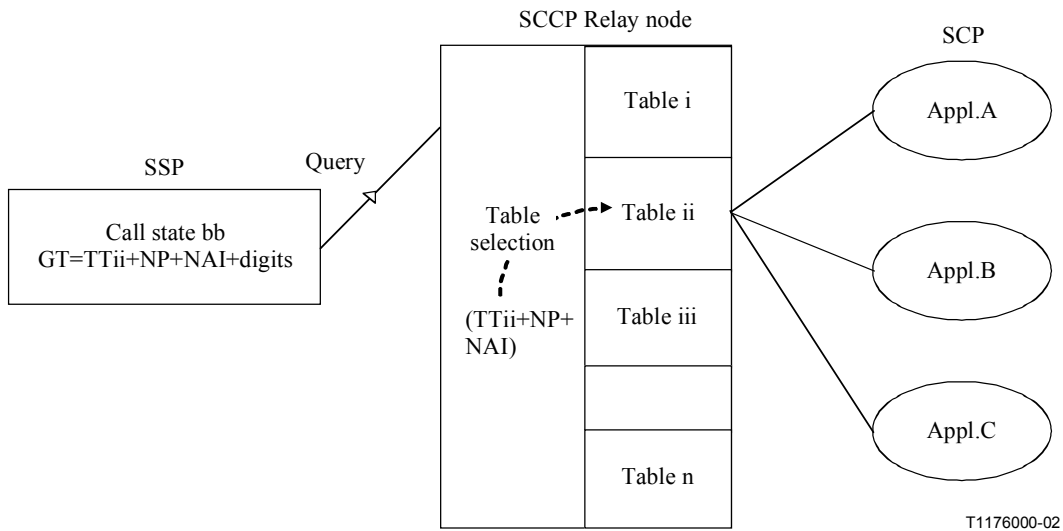


Figure 2/Q.715 – Example 2 of translation type use (CdPN)

Example 3 – An SSP triggers a query to be sent using the called party number (CdPN) as GT. It is assumed that the service offered during the call state "cc" is different from the one offered during the call state "bb" in Example 2. Since the services from the different call states are using the same NP/NAI/GTAI, different translation types will again be required to uniquely identify the different uses of the same GTAI. See Figure 3.

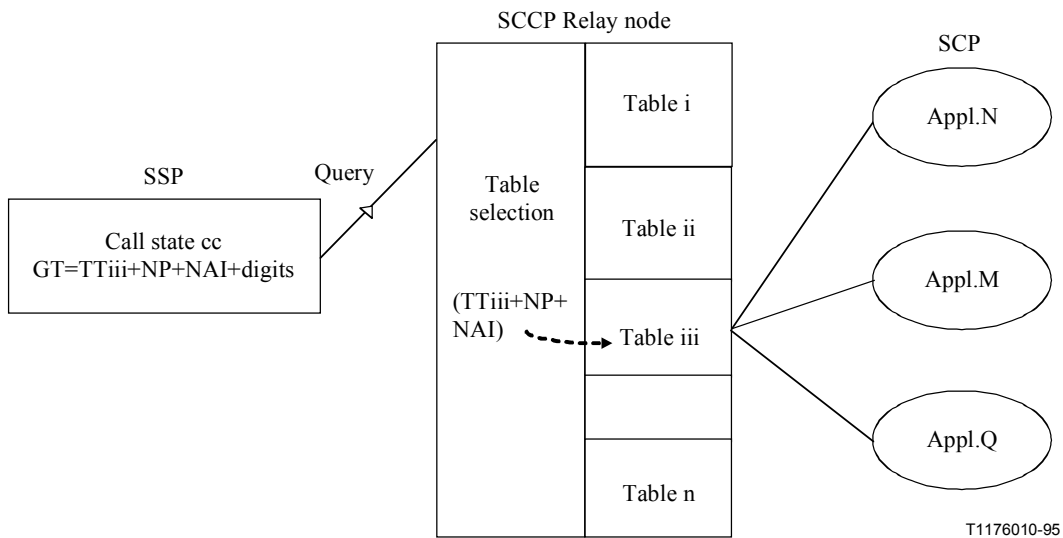


Figure 3/Q.715 – Example 3 of translation type use (CdPN)

Example 4 – An SSP triggers a query to be sent using the billing number (BgN) as GT. Since a new address type is being defined for the same NP/NAI/GTAI as in Example 3, a new translation type is required. See Figure 4.

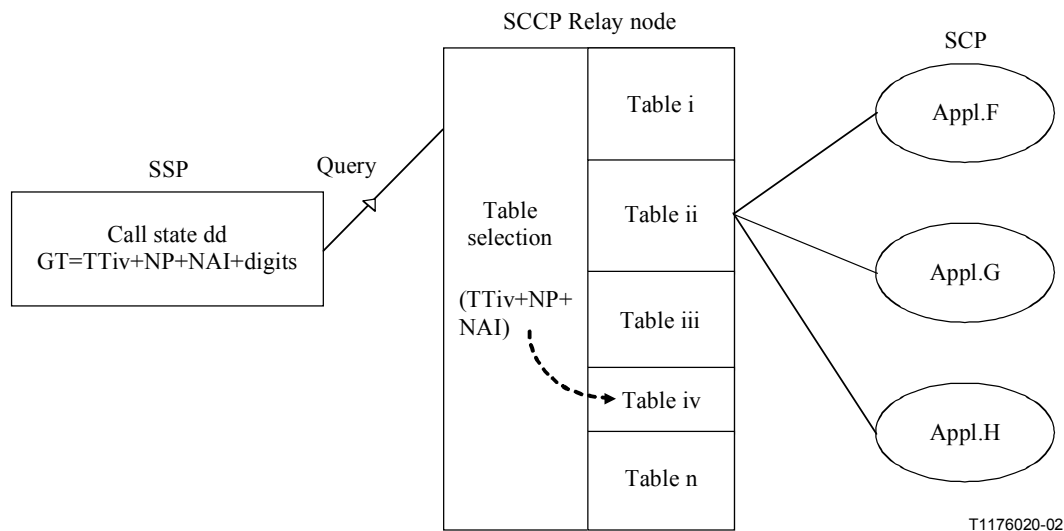


Figure 4/Q.715 – Example 4 of translation type use (BgN)

As shown in the examples above, it is the GTT input and output requirements (translation needs) that are the primary considerations as to when a new translation type is required. The above examples are applicable for all GT-formats in the global title indicator (except GTI = 1).

Examples 1 and 2 show that when the GTs have the same format (i.e. same numbering plan and encoding scheme), different translation types are required to enable the GTT process to produce a different output destination address where identical GTAI digits are employed.

Examples 2 and 3 show that when a previously used digit format (e.g. called party number) is reused for another service, different translation types are again required.

Example 4 shows that when a new address type (e.g. a billing number) is used, a new translation type is required. Note, there are many different billing number formats that can be used (e.g. billing numbers based on E.164, E.118, or some other numbering plan), that may also require a different translation type.

7.1.2.3.3 Translation type assignment guidelines

Based on the examples of the previous clause, the following summarizes the guidelines for assigning translation types:

- 1) For each new GT-format, the characteristics that need to be examined are:
 - a) address type (called PN, calling PN, billing number, unique node-addresses);
 - b) numbering plan (E.164, E.212, etc.);
 - c) nature of the address indicator (if applicable to the numbering plan).

The number of address digits and their encoding should not necessarily require a new translation type value assignment.

- 2) For each reuse of an existing GT-format where an overlap occurs (i.e. overlaps of digit value ranges, preventing a unique translation) a new translation type is required. This also includes the case where there are several generations of a service that require different GTT outputs.

Services can share the same translation type value if their GT-formats are identical and either their use of the address digits within a certain NP does not overlap, or their use of the digits is identical.

Only international services need standardized translation types values to avoid possibly conflicting assignments.

7.1.2.4 Encoding scheme (ES) (3.4.2.3.3/Q.713)

The encoding scheme parameter represents the coding "syntax" of the GT-address, it is as such not a part of the address information. Currently values are assigned for BCD and for a "national specific" format in the context of the "generic numbering plan" OSI-addressing would also allow for IA5 characters or pure binary information to be used as addresses. Encoding scheme values for these and other codings may be specified in future.

7.1.2.5 Global title indicator (3.4.1/Q.713)

The global title indicator indicates the way in which the addressing information is formatted in the message. The most complete format is GTI = 4, which indicates inclusion of the information elements TT, NP, ES and NAI. The other formats contain only some of these information elements, leaving out information that is irrelevant.

- a) GTI = 1 is the oldest and simplest form containing only the nature of address indicator. It was used to send E.164 numbers in BCD format only. In *Red Book* nodes, it is the only available format.
- b) GTI = 2 introduced the translation type to identify particular special types of translations. The information about numbering plan, nature of the address and encoding scheme is to be derived from the translation type.
- c) GTI = 3 includes the numbering plan, in addition to the translation type. With GTI = 3, SCCP can route messages in networks with different numbering plans (e.g. mobile).
- d) GTI = 4 includes the numbering plan, the nature of the address indicator and also the translation type. Its use is prescribed for international interconnections. (See Annex B/Q.713.) Interworking between this format and a national format of GT may have to take place in gateway nodes, when nationally another format is prescribed (e.g. GTI = 2).

7.1.2.6 Digits/global title address information (GTAI) (3.4.2.3.1/Q.713)

Digits can either be:

- numbers derived from the digits dialled by a subscriber or from his/her subscription number (e.g. directory number);
- or addresses that are specifically reserved to identify a certain node or service.

In addition to Binary Coded Decimal (BCD) coded digits, the GTAI field can carry other types of information elements (IA5 characters, pure binary addresses), as indicated by the encoding scheme. (See 7.1.2.4.)

7.1.3 Use of non-standardized TT and SSN in the international network.

Some combinations of standardised/non-standardised SSNs and/or TTs can be used into and across the international network, providing specific agreements are made among network operators.

The TT is a selection key of the translator selector used to differentiate between the use of identical NP/NAI/GTAI combinations (for more information refer to 7.1.2.3). It is used in each node performing GTT. Therefore, the use of non-standardised TTs requires specific agreement among networks that perform GTT.

The SSN is not used for routing purposes. It is used in the final destination node to address the appropriate SCCP-user (for more information refer to 7.1.1). Therefore, the use of non-standardised SSNs requires specific agreement between end networks to assure the correct SSN is derived. Agreement could also be made among networks performing GTT to derive an appropriate SSN in a translator node.

Table 1 below indicates whether specific agreement is needed for various combinations of standardised/non-standardised SSN and/or TT.

Table 1/Q.715 – Nature of agreement needed for types of SSN or TT used

| SSN | TT | International Transit Networks agreement | End Networks agreement |
|------------------|------------------|--|------------------------|
| Standardized | Standardized | N | N |
| 0 | Standardized | N | N |
| Non-standardized | Standardized | N | N |
| Standardized | 0 | N | N |
| 0 | 0 | N | Y (Notes 1, 2, 3) |
| Non-standardized | 0 | N | Y (Note 3) |
| Standardized | Non-standardized | Y (Notes 2, 4) | Y (Notes 2, 3) |
| 0 | Non-standardized | Y (Notes 2, 4) | Y (Notes 2, 3) |
| Non-standardized | Non-standardized | Y (Notes 2, 4) | Y (Notes 2, 3) |

N No specific agreement needed
Y Specific agreement needed
NOTE 1 – GTAI must allow the SSN to be derived at the last translator node.
NOTE 2 – Agreement is needed among networks that perform GTT using the listed TT values.
NOTE 3 – Agreement is needed to assure the correct SSN is derived at the last translator node.
NOTE 4 – Agreement could be used to assure the correct SSN is derived at the last translator node.

7.2 Procedure to derive SCCP-addressing requirements

ITU-T Recs. Q.711 [1], Q.712 [2], Q.713 [3] and Q.714 [4] provide a procedural framework to enable each application to define its application specific global title addressing scheme. Any new application requiring to use the SCCP global title addressing capability will need to go through the same specification process. In the following, a number of considerations or guidelines to specifying the global title for an application are given:

- 1) A high level description of the service ("stage 1") or application including the major relevant features should be available to the Working Party responsible for the global title specification.
- 2) A summary of the stage 2 service description should be available to the Working Party responsible for the global title specification. Major items of relevance are as follows:
 - a) The functional model should clearly-define the functional entities, in particular, entities that may become SCCP addressable destinations.
 - b) Information flows of the functional model should clearly indicate the sources and destinations of the flow.
- 3) A summary of the stage 3 signalling requirements, specifically of the SCCP-user, should be available to the Working Party responsible for the global title specification. While stage 2 descriptions provide the insight to the functional model, functional entities and information flow of the application, the stage 3 signalling requirements provide the definitive requirements to enable specification of the global title.
 - a) The SCCP-user signalling flows or relations, which should correspond to certain information flows of the stage 2 description, should be identified to determine the SCCP user's message destinations and sources.
 - b) How the user messages in each SCCP user's signalling flows, identified in "3 a)", should be routed: based on global title or point code (or both), should be specified.

- 4) Determine whether an existing global title specification for some application is readily applicable to the new application. A few points for consideration are as follows:
 - a) Is the global title address information of that existing application available at the source nodes of the new application?
 - b) Is the global title address information of that existing application capable of identifying the destination entities of the new application?
 - c) Does the new application use a specific range of the global title address information that is not used by another existing application?
 - d) When the existing application and new application share the same range of global title address information, can the final destination entities of these existing and new applications be identified at the application level (e.g. different application contexts, see ITU-T Rec. Q.775 [6] for guidance on this)?
- 5) For a new addressing specification, the addressing criteria to identify all the SCCP addressable destination entities in the application should be identified or established. Some criteria may be listed as follows:
 - a) Is it required to distinguish one country from another one?
 - b) Is it required to distinguish one network operator from another?
 - c) Is it required to distinguish one type of destination "functional entity" from another?
 - d) Is a given global title address information required to distinguish one and only one destination entity from another destination entity of the same type?
- 6) The information, which is available at the source nodes of the application and meet the addressing criteria of 5) should be identified. The information, which is available at different sources, may follow different numbering or identification plans. This information will become the global title address information.
- 7) The TT, NP and NAI should be assigned as appropriate for the global title address information.
- 8) The portion of global title address information that will have to be translated to identify the destination country, destination network or destination entity should be specified.

The results of considerations 1) to 3) include the background information, input and assumptions, which are needed prior to the specification of the global title for the new service or application. Considerations 4) to 8) provide some guidelines to evaluate the composition of the global title.

7.3 Global title conversion operations

SCCP global title translation allows the derivation of a new or modified GT' during the translation of a GT. This capability can for example be used to strip off the country code when a message enters a national network, but also to replace or delete digits. It must be clear that only in very rare cases the complete received GT will be replaced by another. Normally, during digit translation only a few digits of the full GT are analysed, and based on that, a decision is taken how to modify the GT. The modifications need not necessarily be restricted to the part analysed. Whereas the actual implementation details and capabilities of the conversion may be strongly implementation dependent, an abstract model can be used to illustrate the kind of modifications that are possible in the process of modifying the GT. In general, the modification can be represented as a list of simple operations to be executed sequentially on the GT-digits. In addition, these modifications may also lead to a change of numbering plan, translation type, nature of the address indicator and/or encoding scheme.

A possible set of operations is:

- replacement of NP;
- replacement of NAI;
- replacement of TT;
- replacement of ES;
- changing of the GTAI digits: starting with the first digit, the global title conversion functions execute an arbitrary sequence of the following actions:
 - delete a number of digits from the GTAI;
 - insert a number of new digits in the GTAI;
 - pass transparently a number of digits from the old GTAI into the new;
 - replacement of a digit by another digit can be viewed as the combination of a single-digit delete and insert at the same place.

When no more actions are specified, the remaining digits from the old GTAI are taken over unchanged.

7.4 The generic numbering plan

The generic numbering plan was first introduced to support the ITCC service. It can also be used for other services. The "generic number" is composed of an international and a national part. The international part consists of an international SPC (ISPC) defined in ITU-T Rec. Q.708, represented in BCD format. To arrive at an even number of digits, a zero filler is inserted behind it. The national part consists of information that is purely national-significant. It can have either BCD or a national-specific encoding scheme. Within the outgoing national networks(s) and the international network, relay nodes or gateways will only analyse the ISPC in order to determine the next SCCP node. See Figure 5.

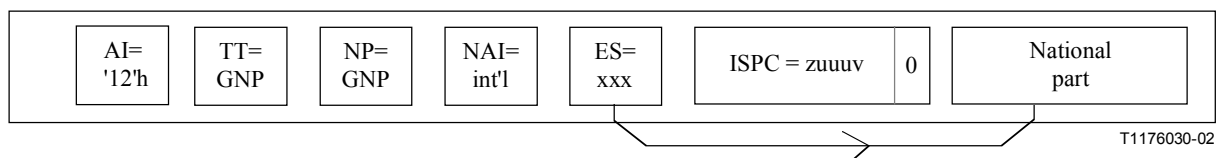


Figure 5/Q.715 – Structure of the generic numbering plan

When both the value of TT or NP refer to the generic numbering plan, it indicates to SCCP that the first six digits are in BCD format, and hence the encoding scheme value must be ignored.

7.4.1 Example

A typical way to provide the national part is to provide the SPC of the node (together with network indicator and SSN if needed).

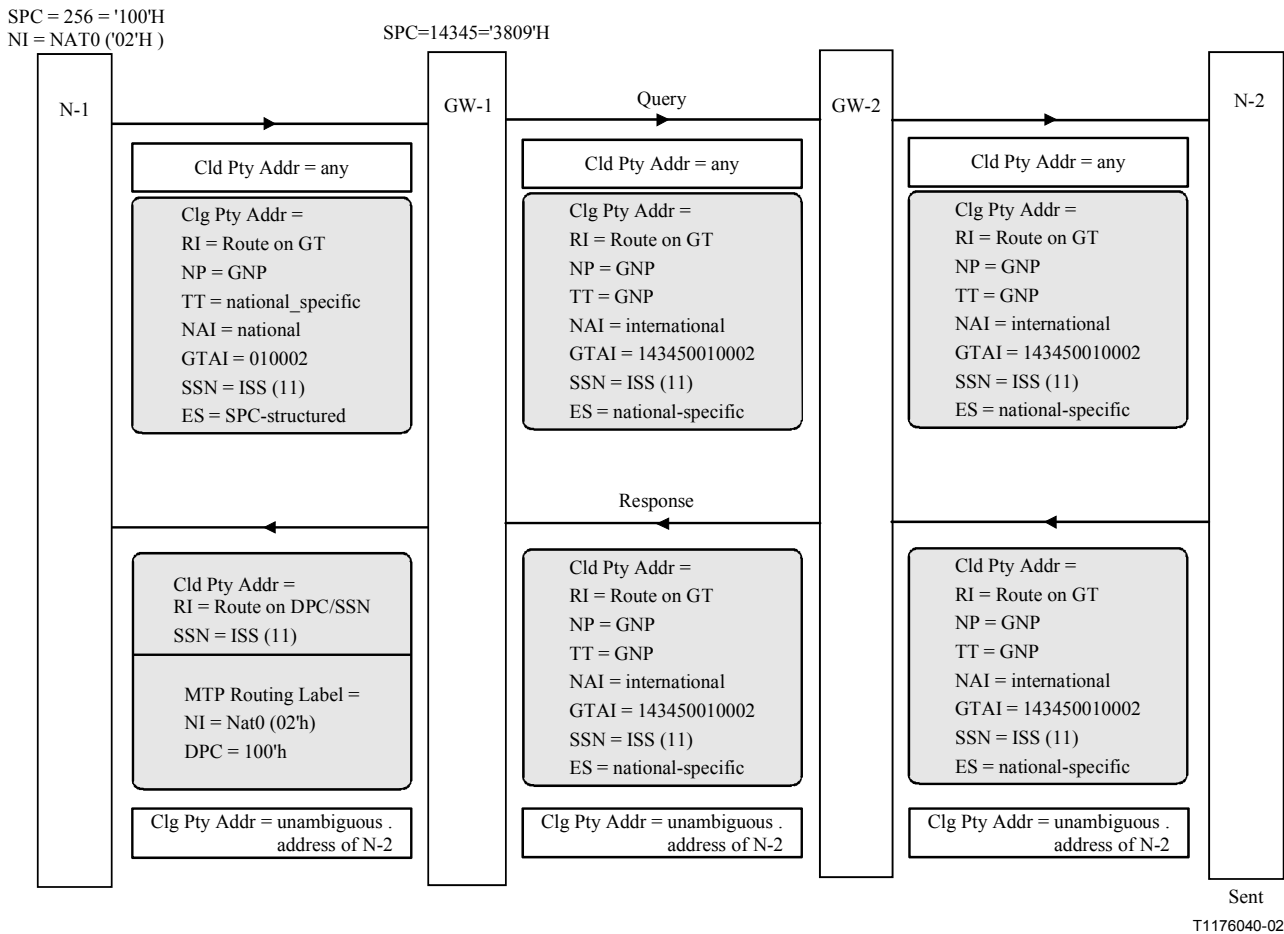


Figure 6/Q.715 – Example for the use of the generic numbering plan

Figure 6 shows an example of the use of the generic numbering plan to provide unambiguous calling party addresses. In the originating national network, a special translation type and encoding scheme are used to indicate the format of the national part, which in this case is composed of the concatenation of SPC and network indicator, both in binary format³. In the outgoing national gateway GW-1, the calling party address is converted by adding the international part, consisting of six digits, representing the ISPC of GW-1, plus one "0" filler digit. NP, TT, NAI and ES are updated. This address is passed to the destination node N-2, which uses it as called party address in the response message. In the destination network, only the international part of the GTAI is analysed to determine an appropriate outgoing gateway capable of routing the message back. Similarly, in the international network, only the international part is analysed to select an appropriate incoming gateway able to route back to the originator of the query. This may not be the same as the gateway originally used to pass the query (GW-1). In the incoming gateway, the GT is now translated. If the network supports full routing on DPC + SSN, this may lead to the DPC + SSN of the originator of the query, and the global title is deleted. Alternatively, the global title may be converted to the national format again.

³ One could also conceive situations where the originating node would not provide a GT in the calling party address and the outgoing international gateway has to convert an address with route indicator = "route on SSN" to a global title address.

7.4.2 Considerations for introduction of the generic numbering plan

- Before using the generic numbering plan, the national part must be specified. In countries with multiple operators, this is the responsibility of some national regulatory body. The rules specified by this body are mandatory to all operators in that country.
- In the case that the SSN and TT are zero (0), then it is necessary to carry an SSN incorporated in the national part of the GTAI.
- A modification of the calling party address to add the international portion makes the message longer by at least three octets. In this way, a message could become longer than the allowed 272 octets and has to be discarded. SCCP does not provide a mechanism to segment such messages in relay nodes. As a result, if possible, provision of sufficient space for an eventual increase of the message length should be made at the originating node.

7.5 Considerations for the SCCP users on the inputs for global title

According to the model for global title translation (see 2.4/Q.714), the GTI is an input for the global title translation. Further, the values for the translation type are not unique, but only valid in the context of one GT-format. For example, for GTI = 2, TT = 4 can mean something completely different than for GTI = 4.

Therefore, it is up to the user to indicate, for example through the absence or presence of some of the addressing information elements, under what GT-format a particular translation type has significance.

Where necessary, the SCCP can convert the format given by the SCCP user to the format preferred in a certain network domain. The mapping rules to convert one GTI into another GTI has to be considered implementation dependent.

8 SCCP networking aspects

8.1 Network structures in view of SCCP management capabilities

This clause discusses a number of network structures that can be built up using the current capabilities of SCCP management as specified in clause 5/Q.714. The text has in the past (up to the 1993 edition) been somewhat open for interpretation, by such sentences as:

"...This allows addresses that are specified in the form of a global title to be translated to different point codes and/or subsystems depending on network or subsystem status"

"...Traffic related to a specific SCCP user may be split among several nodes/subsystems. Under normal conditions, each portion of the traffic is routed to a preferred or "primary" node/subsystem"

The use of any of the capabilities below do not require any extra action on the part of the application, but can be established purely through engineering of the GTT-data.

For definitions of some of the terms used, see 3.1/Q.715.

8.1.1 Configurations of subsystems

8.1.1.1 Solitary subsystems

See Figure 7.

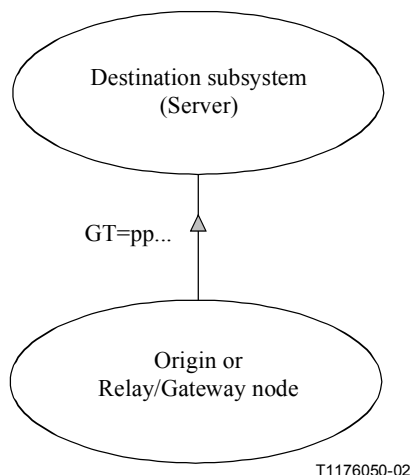


Figure 7/Q.715 – Solitary subsystems

Solitary subsystems are the most easy to manage. If the destination is unavailable, no more traffic is possible; if the node resumes, traffic is possible again. Solitary subsystems are used when the communication is end-to-end between two specific SCCP nodes (e.g. for ISUP or ISDN-supplementary service CCBS), or when the service that is addressed is not extremely important.

8.1.1.2 Replicated subsystems

When a service supported by SCCP is especially important to the operator, duplication of the SCCP subsystem service may be desirable. This will help assure that subscribers will continue to be served in face of equipment failures, scheduled maintenance activities, physical damage to the equipment's site, etc. Several architectures to provide the duplication of a service can be distinguished (this list is not intended to be exhaustive):

- Active/Standby pair (one passive backup serves one primary node/subsystem).
- Centralized backup (one backup node serves many primaries).
- Active/Active pair (two primaries serve as backup for each other).
- Decentralized backup (backup provision is distributed over a number of other, equally active, nodes).

8.1.1.2.1 Active/Standby pair

See Figure 8.

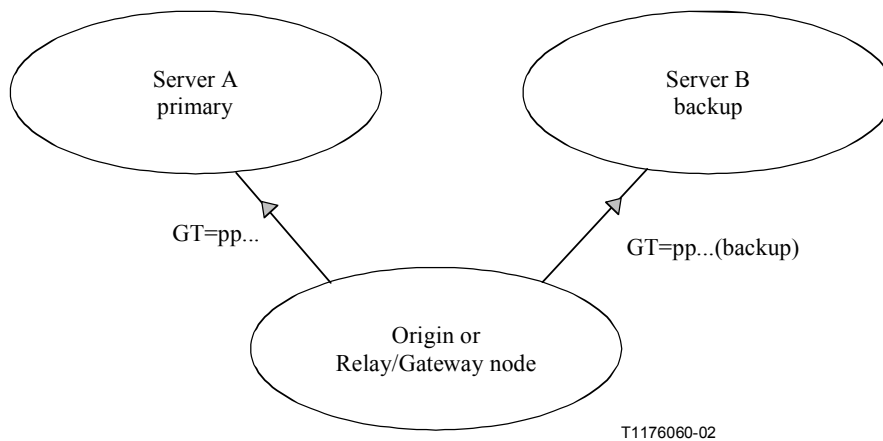


Figure 8/Q.715 – Active/Standby configuration

The most obvious architecture for replicated subsystems is the active-standby pair. In this configuration, the primary node is active, carrying all of the traffic destined for the active-standby pair, whereas the standby is in an idle state until it has to take over traffic from the currently active subsystem. When the primary subsystem goes down or is intentionally taken out of service, the standby takes over until the primary subsystem is restarted.

It should be noted that this architecture doubles the resources needed. Also during overload there is no opportunity to divert load to the backup.

8.1.1.2.2 Centralized backup provision

See Figure 9.

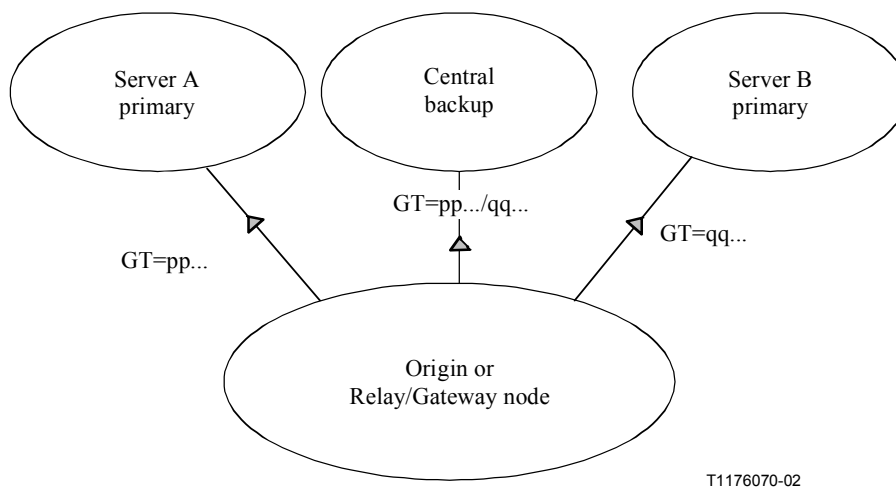


Figure 9/Q.715 – Centralized backup

The service is provided by a number of servers. The traffic is distributed over the servers through the administration of global title translation at the originating/relay/gateway node. Different groups of global titles are assigned a different "primary" destination. When one of the primaries fails or is taken out of service, the traffic is rerouted to one central backup (which must have a copy of the complete databases of all its primaries). This backup is normally in an idle state when all primaries are in service.

This system is compatible with the coordinated state change procedure as long as only "dominant mode" is applied. Each primary can ask the central backup if it is ready to take over some more traffic. The backup will refuse this if it is already overloaded, for example because it is already handling backup traffic for other nodes/subsystems. When service from the primary is restored, the primary automatically takes over again.

8.1.1.2.3 Active/Active pairs

See Figure 10.

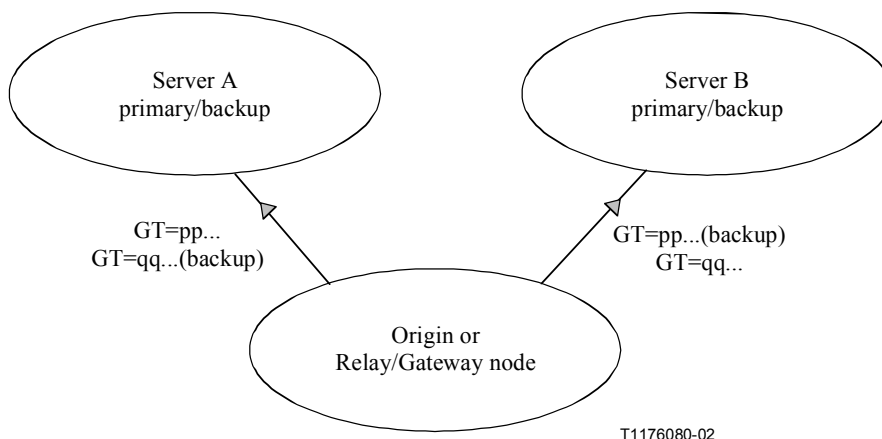


Figure 10/Q.715 – Active/Active pair

In this case, each replica is serving a part of the traffic (e.g. each serving half of it). Load is distributed over the servers through the administration of the global title translation (or by active loadsharing, see 8.1.3) at the originating/relay/gateway node. When one server fails, the other server takes over the load in addition to its own. As soon as the first server is restored, the traffic is redistributed again. This architecture has the advantage that the spare capacity can be employed during overload situations to serve more traffic.

Note that through administration of the GT translation, one source might send traffic to server A as primary, and another source to server B as primary (see Figure 11).

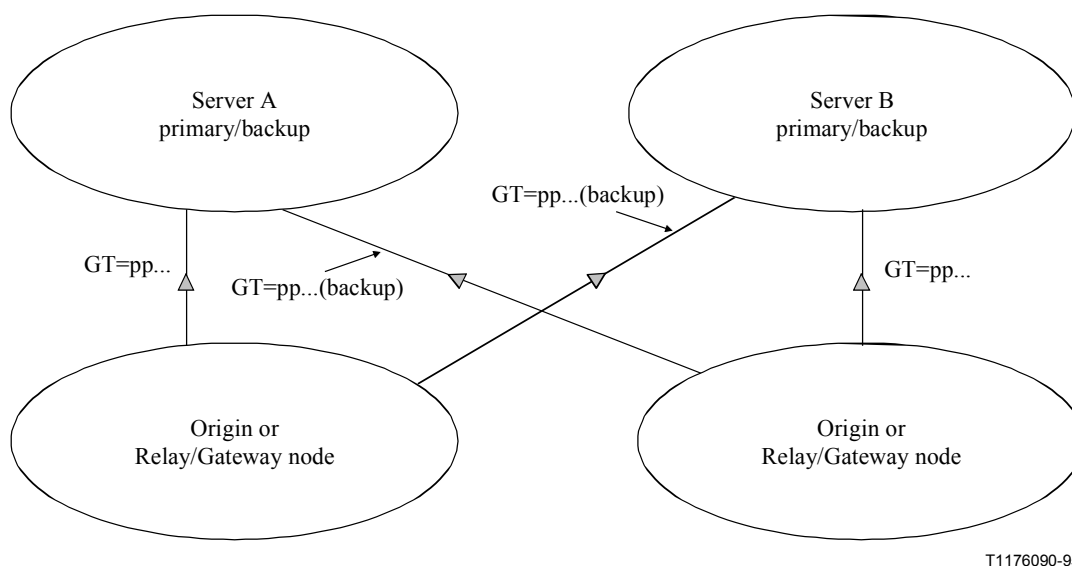


Figure 11/Q.715 – Active/Active pair, geographic specialization per origin

8.1.1.2.4 Decentralized backup provision

See Figure 12.

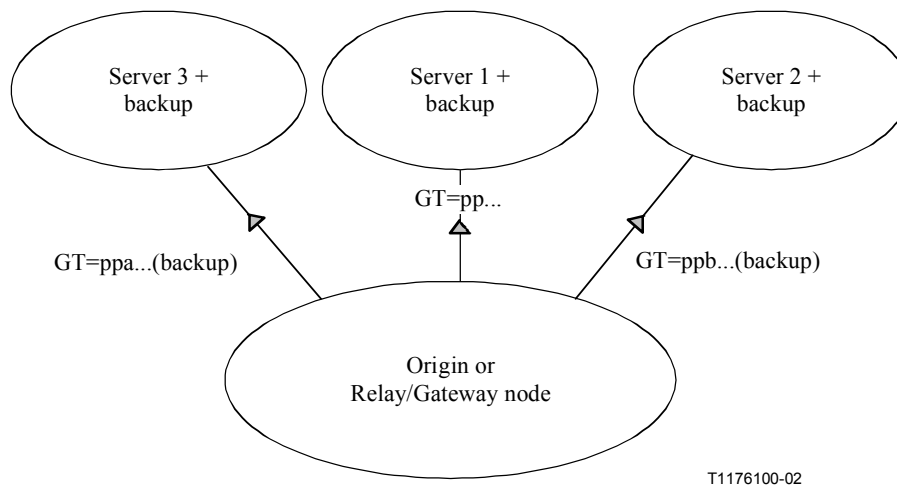


Figure 12/Q.715 – Decentralized backup

It is possible to distribute the backup capability for one node by using several other nodes. This can be arranged by splitting the global title translations towards one node in groups that have the same "primary" but different backups. In this way, when a primary goes down or is taken out of service, the traffic is redistributed over the different backups such that each only has to handle a slightly higher amount of traffic.

This system is, however, not compatible with the coordinated state change procedure as it exists currently. If necessary, the coordination of the state change could be provided through a TMN operations system. Nevertheless, this system may prove to be the most cost-efficient, since it requires only 1/N spare capacity, which is also usable as spare capacity for overload situations.

8.1.2 Unambiguous¹ addresses

Whenever some kind of replicated architecture is used, it is necessary to provide each of the subsystems with its own unambiguous network address. Indeed, whereas the first message within a communication is subject to distribution, the following messages should not be. To illustrate this:

- Assume that a primary subsystem is out of service.
- A new transaction is set up with a GT. The resulting messages will be diverted to the backup.
- Now the primary comes into service again.
- The subsequent messages with the same GT would now be routed to the primary, but the primary does not know about the transaction.

To cater for this, during the transaction set-up, the server that is reached sends its unambiguous network address back to the originator, which should then use it for all subsequent messages (For TC-users, the management of the addressing information will be done by TC, see 3.2.1.6/Q.775 [6]). The unique addresses may be allocated within an existing numbering plan (e.g. E.164), or use the "generic" numbering plan specifically reserved for it. An unambiguous address shall never be translated to a replicated destination. See Figure 13.

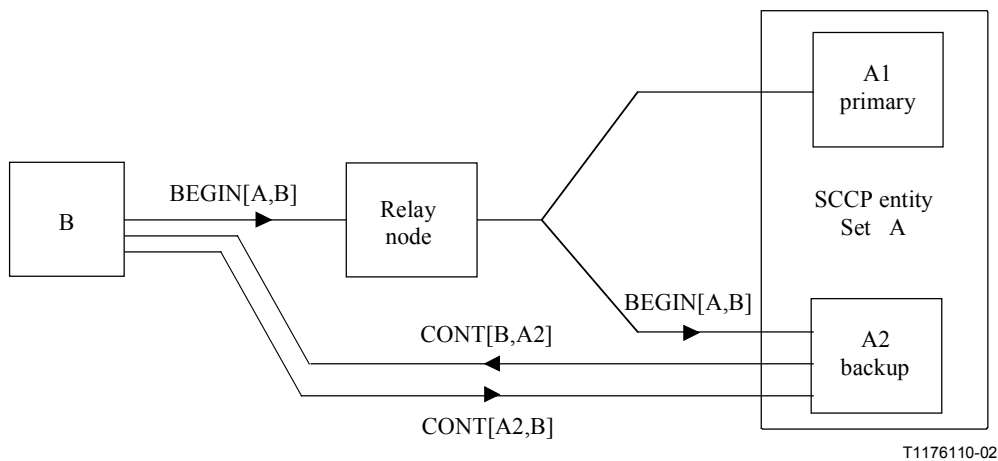


Figure 13/Q.715 – Addressing mechanism for TC based application, example

There are two ways of providing the "unambiguous addresses":

- By reserving specific digit codes within an existing numbering plan, like E.164. An example for the coding can be found in Figure B.4/Q.713.
- Use can be made of the "generic numbering plan" defined and developed specifically for the purpose of identifying individual SCCP nodes or subsystems in a network. The philosophy behind this numbering plan is that within the international network, only the international part (the "Q.708-portion") needs to be analysed to determine the region, operator and node address of a destination gateway. The remainder of the address (called "national part") needs only to be analysed in the network of the destination gateway. The population of the "national part" is therefore entirely the responsibility of the originating national network. Any information can be present.

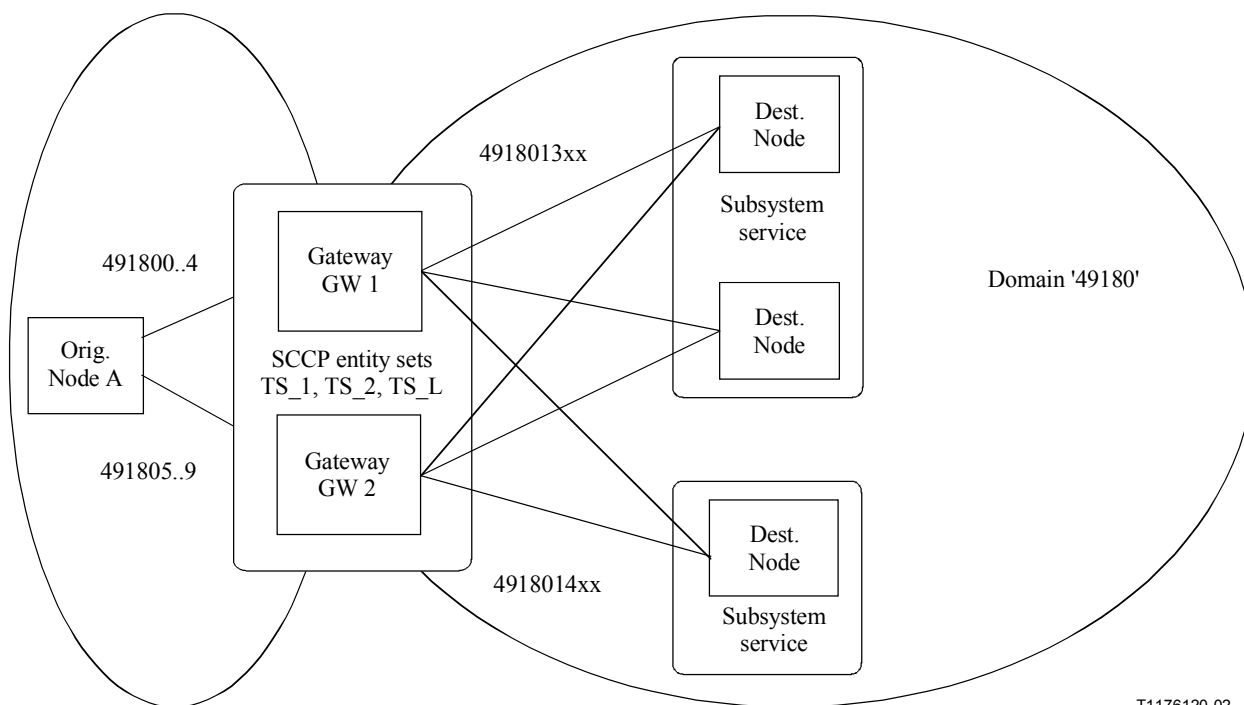
A list of compatibility problems occurring when the "generic numbering plan" is introduced can be found in 6.2.3.13.

8.1.3 Load distribution

Load can be distributed over a number of servers by:

1) *Static load division*

This is done by appropriately engineering the digit translation tables. This approach has disadvantages however, especially in the case of interworking with other operators. This is illustrated with an example. See Figure 14.



T1176120-02

Figure 14/Q.715 – Example of loadsharing

A national operator in country "49" wants to set up a gateway to a private network with CC-NDC = "49180". Two gateways are required and, in addition, each gateway needs a backup. One way of doing this is to create two SCCP entity sets, the first "TS_1" having gateway 1 as primary and gateway 2 as backup, the second "TS_2" having gateway 2 as primary and gateway 1 as backup. The normal load (i.e. the load when both nodes 1 and 2 are operational) must be evenly divided over both "entity sets". To that end, the numbers "491800xx".."491804xx" are assigned to TS_1 and "491805xx".."491809xx" to TS_2, and the translation tables in A are engineered accordingly.

The result might be that 100% of traffic goes to GW_1, 0% to GW_2: because the operator of the "49180" domain started allocating numbers for "service subscribers" such that the GTs are all in the 491801xx range. To overcome this problem it is necessary for:

- a) operators to exchange information regarding the allocation of numbers in their domain;
- b) operators to monitor the use of these numbers and regularly change the translation tables to reflect actual traffic patterns;
- c) extra digits to be translated at the origin or relay nodes or gateways to perform the load-division, which results in processing delays and hence the installation of more equipment than needed.

2) *Active loadsharing*

An active loadsharing mechanism that does not make any assumption on the frequency with which certain global titles are used is desirable. In an active loadsharing scheme, load would automatically be distributed evenly over a single SCCP entity set "TS_L" in loadshared mode, made up of gateways 1 and 2. For each global title translation of "49180" another element of the entity set would be chosen. It is clear that this is an attractive proposition for the operator, relieving the operator from the task of continuously managing the translation tables in close cooperation with other operators.

Loadsharing can be applied to "subsystem groups", i.e. SCCP entity sets consisting of subsystem replicas that are able to provide the same application service for the same group of "service subscribers", as well as to "translator groups".

8.1.4 Configurations of relay/gateway nodes

8.1.4.1 Solitary relay/gateway nodes

See Figure 15.

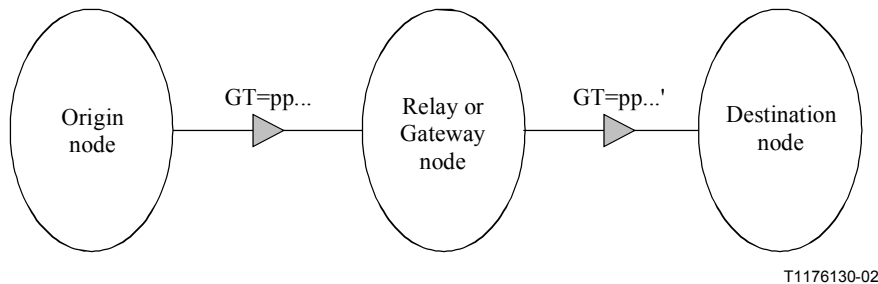


Figure 15/Q.715 – Solitary relay/gateway node

With a solitary relay/gateway node, the origin (or a prior translation node) sends all occurrences of global titles $GT = pp$ to the same translator node for further routing. When that relay/gateway node fails, no backup is provided, and messages for that global title can no longer be delivered to the destination.

8.1.4.2 Replicated relay/gateway nodes

See Figure 16.

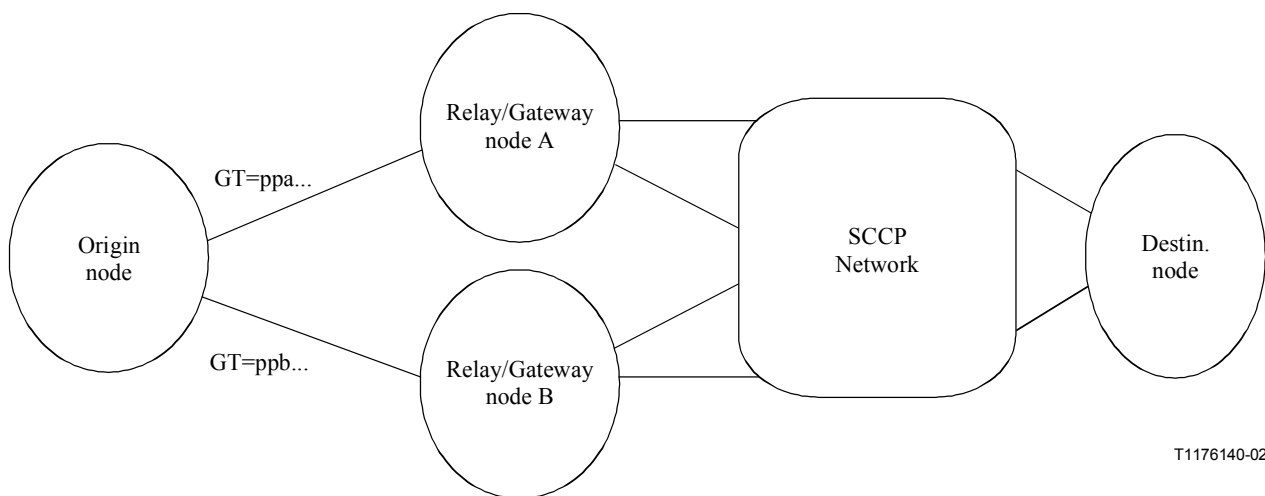


Figure 16/Q.715 – Network with replicated relay/gateway nodes

Load can be distributed over pairs of relay/gateway nodes in much the same way as over subsystems. One way to achieve this is by dividing the global titles in more or less equal groups each being handled by different relay/gateway nodes (which have each other as backup). Another possibility is active loadsharing. In this case, the implementation must make sure that protocol class 1 messages with identical SLS are kept in sequence if they share the same origin and destination addresses.

8.2 Application of connection-oriented services

8.2.1 Coupling of connection sections (clause 3/Q.714)

- 1) Coupling of connection sections is, as a minimum, required in gateways when MTP-network borders are crossed: indeed the connection confirm message (CC) and all

further messages will be routed using the DPC of the other end of the connection section as address.

- 2) Within an MTP network, coupling may be necessary when not every node contains complete MTP-routing tables for all other nodes in the network. MTP routing tables of a local exchange might only contain entries for its immediate neighbours and its transit exchange/STP, but no local exchanges that are connected to other transit exchanges/STPs. To solve this case, in general, a relay node should retain knowledge about every MTP-signalling relation in the network. Then, when a message is routed, the relay node can check whether the node that the message originated from, and the node for which the message is destined, are able to communicate with each other directly. This is a quite large, possibly unmanageable amount of data that has to be kept in every relay node.

Simpler approaches may be feasible:

- Employ coupling throughout the network in every relay node, which is the simplest but not necessarily efficient method.
- Check the DPC and/or OPC only: this gives a pessimistic outcome, since coupling could only be avoided if that OPC or DPC is able to communicate with all other nodes connected to the relay node. This may be the case for example for SCPs. A nearly equivalent approach is to derive the need for coupling from the output of the global title translation (although the problem is related to the connectivity of the MTP network, and is not an SCCP item).
- Divide all nodes into groups, within which intercommunication is always possible. When a message is routed from a node in one group to a node in another group, connection sections are created. However, a group may have signalling relations with many other groups: for example, local exchanges may not only communicate within the group of local exchanges connected to the same relay node, but also with SCPs and other types of equipment.
- Assign all nodes to groups and retain a table of which groups can communicate with other groups. Again, this may become difficult to manage.

As can be seen, it is difficult to establish one criterion that is valid for all network configurations. Two factors should be carefully weighed against each other:

- a) the gains that arise from not coupling connection sections: less occupancy of resources in relay nodes, better transit delay times.
- b) the amount of effort to manage the administration arising from very general or very sophisticated solutions.

8.3 Application of connectionless services

8.3.1 The return on error procedure (4.2/Q.714)

SCCP provides the return on error procedure as a means for the application to be informed about messages that SCCP cannot route to the end-destination. In certain circumstances the XUDTS, LUDTS or UDTS messages that are used to inform the originator can be mis-routed. Implementors, application specifiers and Administrations alike should be aware of this and should not rely solely on it for managing SCCP routing problems, although the procedure should still be considered useful. Applications should have built in mechanisms to deal with end-to-end communication loss and not rely solely on the SCCP return on error procedure.

The following subclauses of clause 8 give examples of possible problems occurring with the return option.

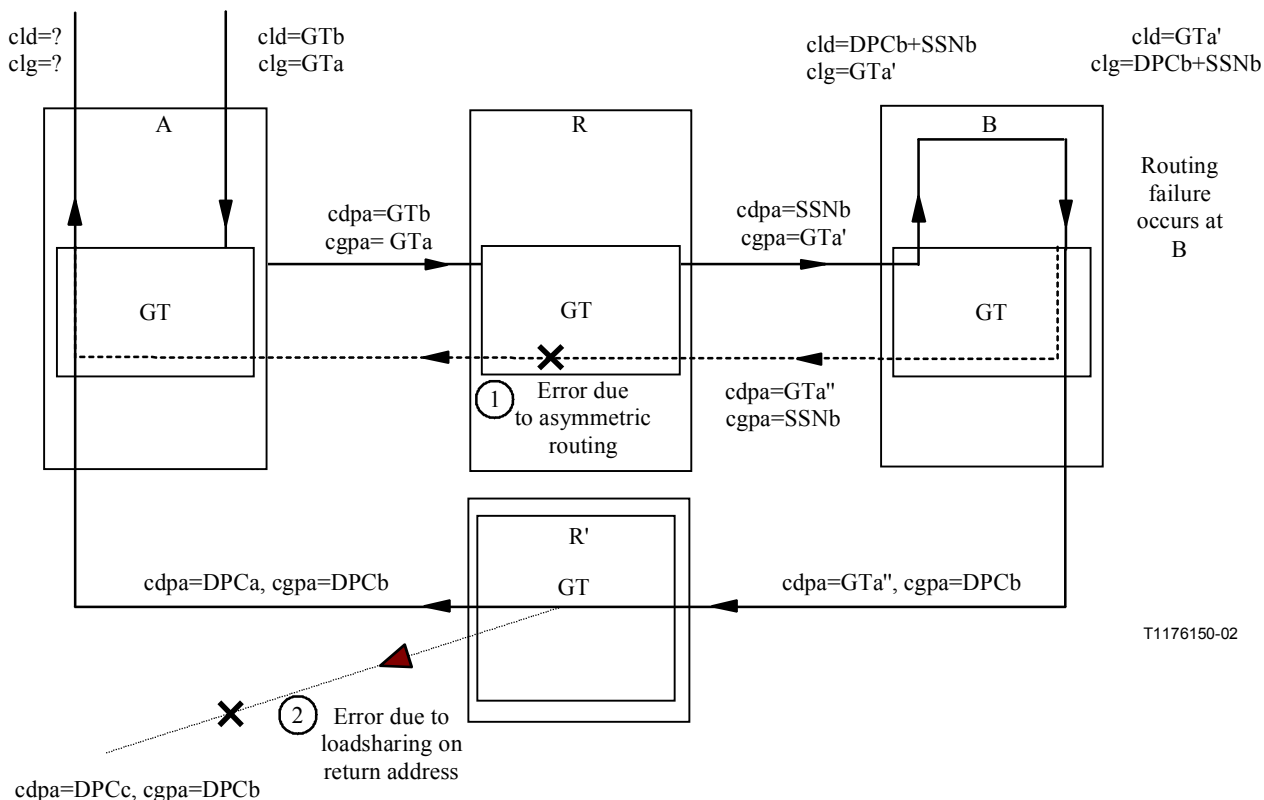


Figure 17/Q.715 – Example of message flow for return option in SCCP connectionless service

8.3.1.1 Incomplete routing

If a message is received from a relay node, that relay node is not necessarily able to translate the called party address of a message returned to it (formed from the calling party address of the forward message, see Figure 17). All nodes that may be required to return messages due to invocation of the return on error procedure must first perform a normal GT translation on the called address of the message to be returned (i.e. as it would when originating a message under normal circumstances) in order to identify the correct node to send the message to and not simply return the message to the node from which the forward message was received.

Every node on an outward route must know a valid route on which to return the message. All nodes on the outward route must be configured to be able to perform global title translation of the Global Title Address Information formed from the calling party address of the outward message.

8.3.1.2 Replicated subsystems

The GT in a calling party address ("clg a") of the (X/L)UDT must unambiguously identify the subsystem at node A, so that, when used as the called party address in a (X/L)UDTS, the final translation must not be subjected to backup routing nor loadsharing (otherwise a wrong transaction in the other node might be affected by the received (X/L)UDTS, see Figure 17).

8.3.1.3 Scope of calling party address

The calling party address of the originator ("Clg a" in Figure 14) must be valid in the domain to which the message is finally sent (unless the gateway node offers calling party conversion to complete the calling party address at network border crossing). Care is needed to avoid that an invalid/incomplete address is passed across network boundaries, in order to avoid that the message routed back using this address, disturbs an active connection or TC-transaction in another node. Therefore, the OPC, national SSNs and NP/NAI/TT combinations for which there is no backward

translation table must not be passed if they are not valid in the transited/destination network. A supplementary screening mechanism that at least checks the outgoing SSN and the NP/TT/NAI combination could be considered desirable.

8.3.1.4 Calling party addresses in (X/L)UDTS message

When the routing indicator of the called party address in messages received at end nodes has been set to RI = 'route on SSN', the called party address will then include the SSN of the destination application and possibly the DPC of the end-node. Potentially, these address parameters could then form the calling party address in a returned (L)(X)UDTS message. If the service message has to cross international boundaries, it could be useful to populate the calling party address with only an SSN set to value zero to avoid discard of this message at the international boundary. Also see 2.7/Q.714 for calling party address treatment.

The message delivery problems occur especially if the destination network does not use the subsystem management procedures to inform the relay node of subsystem status changes in the destination node. The problem would also be caused by reassembly difficulties in the end node.

8.3.1.5 GT conversion

When the GT is changed during routing the (X/L)UDT (e.g. to remove the country code from the GTAI), and the return option is applied in a relay node, the calling party address sent back may contain any intermediate result of translation in the forward direction. It would be advantageous if the inverse conversion could be possible in the calling party of the (X/L)UDTS (i.e. reinstate the country code again). This would help sending back significant information. This is not feasible for example, if the stripping of the country code is done in the outgoing international gateway (as is the rule for digit translation in telephony). To achieve a meaningful calling party address, the CC and NDC of a global title should be retained in the international (or other transit) networks.

As 8.3.1.4 and this clause indicate, the calling party address sent back may contain any intermediate result of translation of the called party address in the forward direction. It cannot therefore be used as a reliable indication for any accounting, measurements, traffic management activity or whatsoever, unless it is known that no changes have been made, or sufficient information has been retained.

If screening on calling party address is applied on (X/L)UDTS messages, messages could be blocked because their calling party address is not valid. Also, messages might be rejected or discarded, since the calling party address was originally the called party address in a (X/L)UDT that could not be routed. Perhaps the checking on calling party addresses should be less stringent on (X/L)UDTS messages than on (X/L)UDT messages.

8.3.1.6 Connectionless segmenting/reassembly

When employing segmenting/reassembly, the return option is used to send back XUDTS (or LUDTS) messages whenever the reassembly process fails. In the case of TCAP, the message sent back may not always be deliverable to the correct TCAP transaction when a segment that is not the initial one is returned, since the user data will not contain a transaction ID.

SCCP implementations have an option to decide whether to put the return option on in all segments of a long message, or only in the first. In the former case, one must be aware that under certain circumstances, not all segments are returned, but only a first segment, or an arbitrary part of a message. This is the case when:

- A reassembly error occurs – the destination node then returns a single XUDTS (or LUDTS) message, containing an arbitrary first part of the data already received.
- A LUDT message is returned, but through a path that does not support long messages. In that case, the user data is truncated in order to fit in one single XUDTS (or short LUDTS) message.

- An LUDT message was segmented in an MTP/MTP-3b interworking node. The return option is only carried across in the first XUDT segment sent out. So, only a single XUDTS with the first segment will be returned.

Under these conditions, reassembly of the original user data from the XUDTS (or LUDTS) messages is not possible.

8.3.1.7 Syntax checks

Syntax checks in a relay node are permitted to be less stringent than in end-nodes. Only the "necessary" routing data are required to be checked (see 4.3/Q.714). If the return option is now applied, the danger exists that a message is returned that is corrupted, but gets "repaired" through the reformatting of the (X/L)UDTS message, although containing complete nonsense. It would be advisable to perform a more complete syntax check of the received (X/L)UDT message before using its information to format the (X/L)UDTS message. In addition, called party addresses that are not reliably decodable should be treated as "syntax errors" (as it is now described in 3.10/Q.714). The appropriate action should be to discard them (i.e. not to subject them to the return procedure). Otherwise complete nonsense may be returned in the message, especially in the calling party address.

8.3.2 Maximal length supported by SCCP connectionless procedures

MTP, according to ITU-T Rec. Q.704, 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 255⁴ octets of user data in the UDT or XUDT message. The XUDT message was introduced in the *1993 edition* of SCCP. These figures are under the condition that no global titles and optional parameters are present.

If a user wants to send longer user data, SCCP (from the 1993 edition onwards) is able to transfer this by segmenting the user data in maximally 16 parts and send them in individual XUDT messages. The theoretically maximum amount of user data is then 3968 octets⁵. 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 application message syntaxes.

When the SCCP is enhanced with broadband capabilities (i.e. the *1996* and *2001 editions*), it can transport up to 4065 octets of user data over MTP-3b facilities (ITU-T Rec. Q.2210 [16]) without segmenting, in one LUDT message. However, not all (parts of) a network need provide MTP-3b facilities. SCCP provides interworking functions that allow a long LUDT message to be segmented in smaller parts in relay nodes and transported as XUDT messages. If the application does not have any knowledge about the occurrence of this situation, it should put itself on the safe side and restrict itself to the same possibilities as when no MTP-3b facilities are present (i.e. the safe 2560 octets).

Network operators may want to limit the maximal message length transported in the SS No. 7 network in order, for example, to limit the influence of long messages on transit delays. This is done by administering the value "Z" (see 4.1.1.1/Q.714). This value may be varied between 160 and Y

⁴ 255 corresponds to the maximum length of the SIF (272 octets), minus the fixed overhead of an XUDT message, i.e.: routing label (4 octets), Message Type (1), Protocol class (1), Hop counter (1), Pointers (4), minimal called address (3), minimal calling address (2), and the length field of the data parameter (1) [$272 - 4 - 1 - 1 - 1 - 4 - 3 - 2 - 1 = 255$].

⁵ $3968 = (255 - 7) \times 16$, where 255 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.

(ITU-T Rec. Q.713). The lower limit of 160 will guarantee that 2560 octets of user data can be transported on that network per message (i.e. in 16 segments).

The following table lists the maximum number of octets available for storing addresses and user data in a (X)(L)UDT message for different editions of the Recommendations. Detailed calculations of the octet limit is also given.

| SCCP message | UDT | XUDT | | | | LUDT |
|-------------------------------|----------|--------|-----|----------|-----|------|
| Single/multiple | – | Single | | Multiple | | – |
| Version | 88/93/96 | 93 | 96 | 93 | 96 | 96 |
| Routing label | 4 | 4 | 4 | 4 | 4 | 4 |
| Message type | 1 | 1 | 1 | 1 | 1 | 1 |
| Protocol class | 1 | 1 | 1 | 1 | 1 | 1 |
| Hop counter | – | 1 | 1 | 1 | 1 | 1 |
| CLD pty address | 4 | 4 | 4 | 4 | 4 | 5 |
| CLG pty address | 3 | 3 | 3 | 3 | 3 | 4 |
| Data (Note 1) | 2 | 2 | 2 | 2 | 2 | 4 |
| Optional part PTR | – | 1 | 1 | 1 | 1 | 2 |
| Segmentation (Note 2) | – | – | – | 6 | 6 | – |
| Importance (Note 2) | – | – | 3 | – | 3 | 3 |
| EOP | – | – | 1 | 1 | 1 | 1 |
| Total fixed overhead (Note 3) | 15 | 17 | 21 | 24 | 27 | 26 |
| Maximum user data (Note 4) | 255 | 255 | 251 | 248 | 245 | 4065 |

NOTE 1 – Parameter pointer and parameter length.
NOTE 2 – Parameter name, parameter length and parameter contents.
NOTE 3 – Inclusion of optional parameters.
NOTE 4 – Maximum user data is obtained when the minimum address contents, i.e. 1 octet for calling (address indicator only) and 2 octets for called party address (address indicator and SSN) is used. In case of UDT or single XUDT messages, the user data is restricted to 255 octets.

8.4 Support of MTP-3b

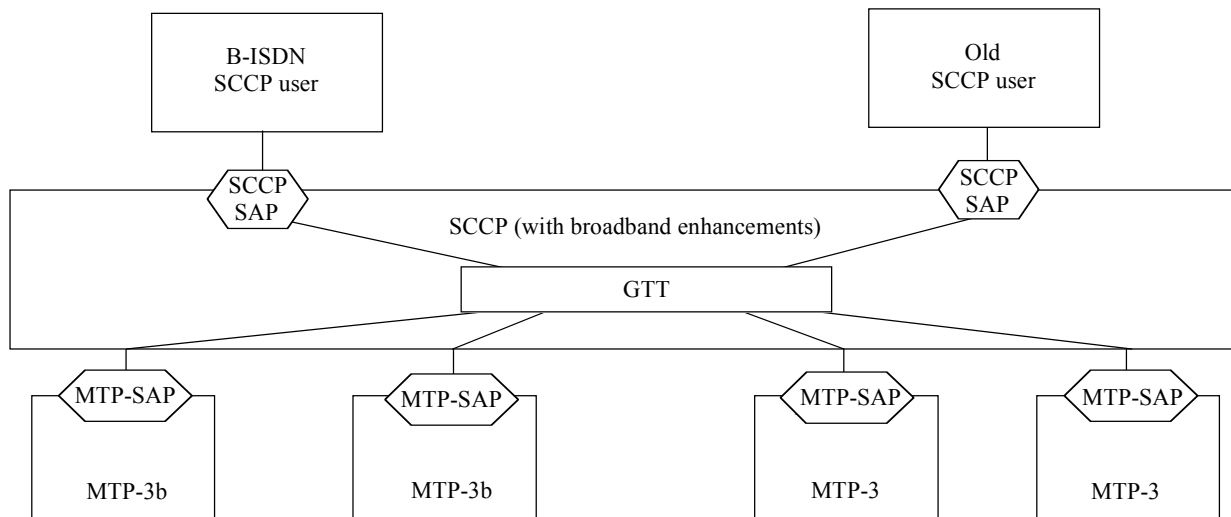
8.4.1 Protocol architecture

To support signalling for B-ISDN, an extension of MTP level 3 (called "MTP-3b", refer to ITU-T Rec. Q.2210) was defined that allows the transportation of large signalling messages via SAAL links with potentially much higher data rates than the MTP level 2, according to ITU-T Rec. Q.703. The SCCP was enhanced (*1996 edition*) 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 use the enhanced SCCP later without any change to the application;
- also existing SCCP users are able to benefit from the new capabilities offered by MTP-3b.

From the user's point of view, there is only one single SCCP entity. The SCCP allows to use a variety of MTP networks at the same time, as shown in Figures 18 and 19. Although currently ITU-T Recs. Q.704 and Q.2210 do not define interworking between them, SCCP can potentially support networks in which such interworking occurs, as shown in 8.4.1.2. It should be noted, however, that in all cases the data transport limits of 8.3.2 apply.

8.4.1.1 Separate MTPs for broadband and narrowband

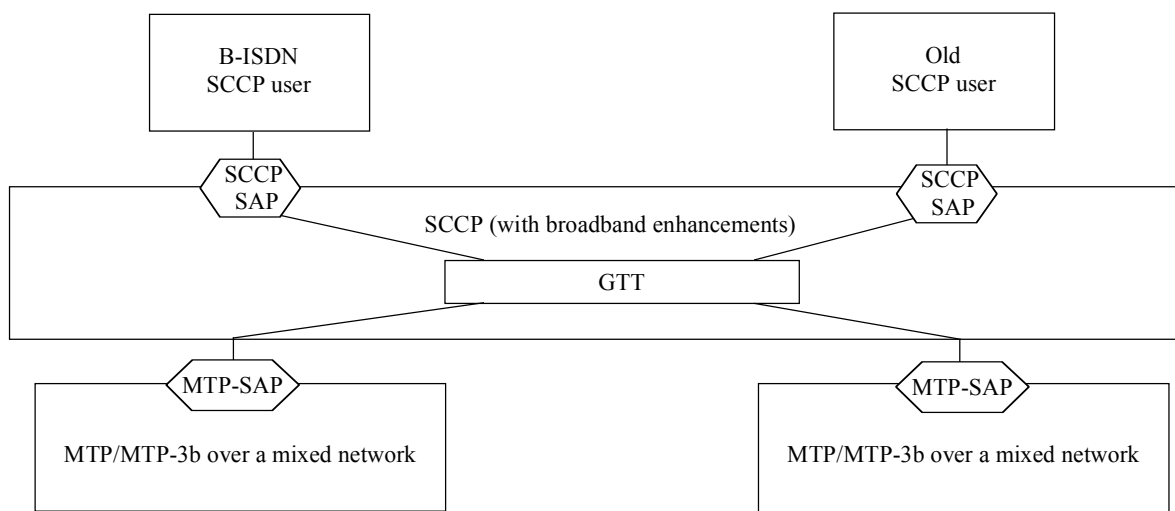


T1176160-02

Figure 18/Q.715 – Separate MTP networks for broadband and narrowband

Here, the narrow-band portions and broadband portions are treated as different MTP networks. Interworking occurs at the gateways where SCCP performs a network boundary crossing.

8.4.1.2 Mixed MTP network



T1176170-02

Figure 19/Q.715 – Mixed MTP networks

In this architecture, mixed broadband and narrow-band MTP exist. 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-SAP alone, whether it is allowed to send a broadband message or not, since the destination could be reachable only via narrow-band links, even though initially the message is sent out from the node over a broadband link. Extra information must be stored against each destination indicating whether it is reachable via MTP-3b or not, and whether the destination can support the LUDT message type;
- in mixed MTP networks, there might be situations where a narrow-band route is used as backup for a broadband route. So, whether the broadband 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.

8.4.2 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 MTP-3b 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 MTP-3b facilities over the signalling route 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 XUDT, XUDTS message types provided in the *1993 edition*, therefore allowing the segmenting of a 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 (see Figure 20):

- 1) interworking at the MTP level;
- 2) interworking at the SCCP level;
- 3) interworking at the application level.

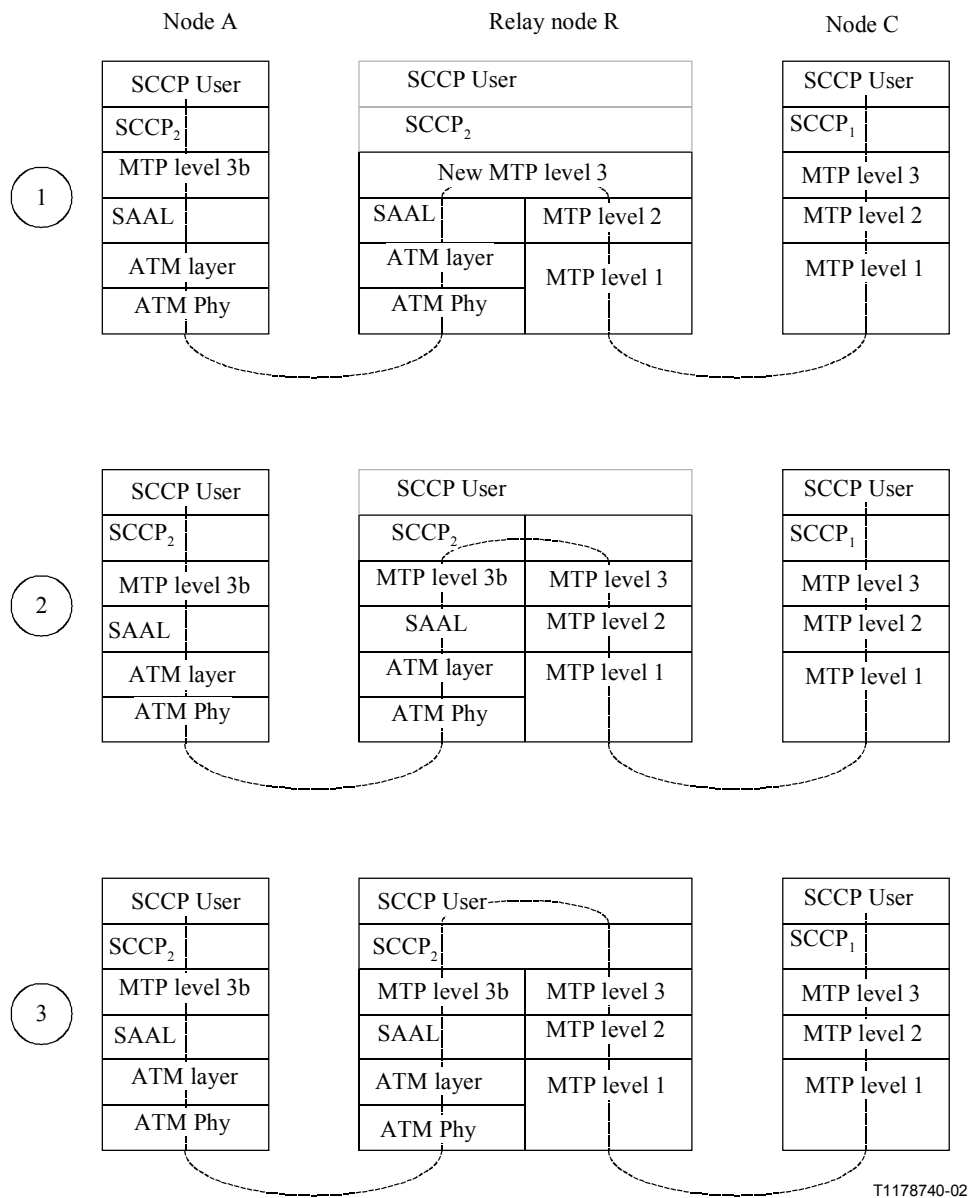


Figure 20/Q.715 – Protocol stacks for different interworking scenarios

NOTE – In Figure 20, the term MTP level-3b refers to an MTP according to ITU-T Rec. Q.2210, SCCP₁ refers to a version of SCCP according to the *1993 edition*, *1996 edition* or *2001 edition* (not necessarily including the extensions for the use of MTP-3b capabilities), and SCCP₂ refers to a version of SCCP according to the *1996 edition* or *2001 edition*, including the extensions for the use of MTP-3b capabilities. 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 narrow-band SAAL links.

8.4.2.1 Interworking at the MTP level

In mixed networks, having a mixture of narrow-band 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 (ITU-T Rec. Q.703) 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.

8.4.2.2 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 broadband capabilities to narrowband ones. The tasks carried out by this interworking node may be:

- conversion of LUDT messages to XUDT messages;
- segmenting long (i.e. the user data of which does not fit into one XUDT message) LUDT messages to multiple XUDT messages.

Optionally, the interworking function might also provide the conversion of a single XUDT(S) to a single LUDT(S) message [but only when no segmenting of the XUDT(S) is needed due to the length increase of the LUDT(S)].

8.4.2.3 Interworking at the application level

Interworking may also be provided by the application itself. The SCCP is, however, 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 narrow-band one or vice versa.

8.4.2.4 Further interworking cases

In practice, combinations of the various situations described will be encountered, especially in the initial stages of introduction of MTP-3b into existing networks.

9 SCCP congestion handling

It should be noted that the timer and restriction level values specified in the SCCP congestion handling procedures (ITU-T Rec. Q.714, 1996, 2001 editions) are tentative until the conclusion of performance studies are known and/or experience is gained in operating the procedures in real networks.

9.1 Assigning importance values to application messages

SCCP (1996 edition onwards) provides congestion control measures to reduce traffic in the event of MTP-congestion, SCCP congestion and SCCP node congestion. It is necessary that SCCP takes these measures on behalf of the SCCP-subsystems, for several reasons:

- The SCCP subsystems may not be able to react to the N_PCSTATE primitives that refer to a certain DPC. If the SCCP subsystems use global titles for addressing, they probably are not able to identify the MTP node concerned.
- Because a relay node cannot pass the congestion notification for remote nodes to the originating node, the relay node must be able to take action itself.
- SCCP must also protect itself and the node it resides in against subsystems that fail to take the necessary measures in case of congestion.

To allow SCCP subsystems to have some control over the actions that are taken, SCCP allows the SCCP-subsystems to assign an "importance" value to each primitive that will lead to data transfer.

So, as a first step, the SCCP user should assign an importance to the concerned application messages. As guidance to the selection of the "importance" value, the message might be assigned to one of the following classes:

- a) messages that, when accepted will give rise to more messages being sent afterwards, e.g. a CR or TCAP:BEGIN message;

- b) messages that are sent during an active connection or transaction and have no predictive value, e.g. DT1 message or TCAP:CONTINUE;
- c) messages that announce the end of a connection or transaction, e.g. RLSD, ERR, or TCAP:END message;
- d) messages on which the working of the protocol is dependent, for example IT or EA.

In the absence of importance values from applications, SCCP will assign default values, see Table 2/Q.714.

For connection oriented users, N-CONNECT primitives are load-initiating, N-DATA are load-contributing and N-DISCONNECT is load-reducing. N-EXPEDITED DATA is an example of indispensable messages.

For TC-USERS, TCAP:BEGIN should normally be considered as load initiating, TCAP:CONTINUE/UNI are load contributing and TCAP:END/ABORT are load reducing.

In general, messages of class A should be marked as less important than those of higher classes, (rejecting a new set-up attempt is in general more acceptable than disturbing an existing one). Nevertheless, this need not always be true. The initial assignment may have to be modified based on the following considerations such as⁶:

- Some transactions may be "follow on" actions that are triggered from another call/connection/transaction. In this case, the TCAP:BEGIN may be assigned a higher importance than normally.
- The end-user for which a connection or transaction is set up may have a high priority (emergency service).
- Congestion actions in SCCP might lead to throughput-fluctuations if the transaction holding times are very short. For such short transactions, the user can smear out the actions over several levels by assigning an importance taken out of a certain range.
- In some cases, a series of messages is sent that must be received all together to avoid failures. If the protocol does not provide safeguarding measures (e.g. by numbering the messages), it may be necessary to give some message types a higher importance than would otherwise be needed.
- If the subsystem itself provides reliable congestion control measures, it can mark the importance somewhat higher to assure that the grade of service is not further degraded by the SCCP network.

Messages reporting application overload indications or containing information elements doing so should get a high importance. The number of such messages must however be kept within reasonable limits.

9.2 Responsibilities for the application

Although SCCP now takes action, it is still better that congestion control is applied end-to-end by the application. The application gets information from SCCP about congestion in two ways:

- 1) through the N_PCSTATE primitives on a destination by destination basis;
- 2) through the reception of N-DISCONNECT, N-INFORM and N-NOTICE primitives, with the reason referring to congestion. The application will normally be able to correlate these primitives with a certain SCCP connection, TC transaction, association and/or end-user and can then take action limited to these.

⁶ These and other considerations might lead to revisions of the definition of the different classes.

When the application is informed about congestion it should whenever possible:

- restrict the sending of messages with importance lower than the congestion level indicated for the destination, in those cases that it is feasible for the application to identify and store information for the destination by SPC;
- apply end-to-end congestion control measures (call gapping, windowing);
- inform its end-user to stop traffic generation. For example when an N-INFORM for a SCCP connection supporting UUS-3 (User-to-User Service 3) is received, ISDN can send a CONGESTION-CONTROL (receive not ready) to the ISDN-terminal to stop the generation of UUS messages;
- when possible, the application shall try to avoid the immediate repetition of messages that were discarded. This may be done by extending the timers that control the repetition of these messages.

9.3 Application of MTP congestion procedures

The mechanism used to reduce traffic consists of rejecting all messages that are assigned a certain importance class below a defined restricted importance level, plus a portion of the messages with importance equal to that restricted importance level.

The effectiveness of the method strongly depends on the mean holding time of connections or transactions: e.g. taking away all new set-up attempts only has an effect after about $0.1 \times T_{\text{hold}}$. For telephony traffic this still is >10 seconds. For short transactions, the method may however be too harsh. However, SCCP has no knowledge about the holding times of the connections or transactions for a certain application. If an application wants to have a smoother method, it can control this by not assigning fixed importance values, but by assigning values selected from a certain range around the mean value. For example, if an application assigns importance values 0..3 uniformly, 25% of traffic is discarded at congestion level 1, 50% at level 2 and so on⁷.

The selection could be random, or it could be based on, for example, a priority assigned to the subscriber being served.

9.4 Application of SCCP and node congestion procedures

Every SCCP implementation must have the capability to react to the SSC messages that are reporting SCCP or node congestion. Whether an implementation itself generates the SSC messages is implementation dependent. According to ITU-T Rec. Q.542, automatic congestion control measures are typically only taken by large digital exchanges and transit exchanges, not by small local ones.

If the local SCCP is overloaded, independent of the rest of the exchange, local measures should be taken to reduce the overload. When the overload situation continues and threatens to influence already established connections or transactions, the SSC message should be sent. Implementations should, irrespective of the availability of the SSC message, be robust enough to keep working under such overload conditions.

9.5 Coordination of congestion control measures between SCCP and other MTP users

When MTP congestion is reported, the MTP status indication primitives are broadcast to all MTP users. All users should take actions then to reduce traffic. This traffic reduction should be more or less synchronized, in order to avoid one user suppressing traffic of another one. As the congestion control procedures of TUP and ISUP leave a lot of room for implementation-dependent decisions, it is not possible to standardize this synchronization. It is hence up to the implementors to make sure

⁷ Assuming the provisional values of 2.6/Q.714.

that the actions taken in SCCP are more or less comparable with the actions taken in TUP/ISUP. This can be done by carefully determining the timers T_a , T_b and the values M and N (see 2.6/Q.714).

Sending of SSC messages reporting node congestion should be synchronized with the actions taken by the node for other MTP users (e.g. automatic congestion control, trunk blocking). An implementation not providing such measures, should also not send the SSC message in the case of node congestion, because the SCCP traffic may be suppressed, while other traffic (that is perhaps causing the overload) continues.

10 SCCP support for Number Portability

For "pure" NP support existing SCCP functionality is considered sufficient i.e. derivation of a new/corrected called address as a result of porting is possible using existing specified SCCP procedures. No use of an external database is necessary provided the corrected address data is stored locally logically to the SCCP routing control function. Specification of functionality to support NP within an SCCP user may require changes to internal SCCP procedures and functions – particularly to internal addressing.

SERIES OF ITU-T RECOMMENDATIONS

| | |
|-----------------|--|
| Series A | Organization of the work of ITU-T |
| Series B | Means of expression: definitions, symbols, classification |
| Series C | General telecommunication statistics |
| Series D | General tariff principles |
| Series E | Overall network operation, telephone service, service operation and human factors |
| Series F | Non-telephone telecommunication services |
| Series G | Transmission systems and media, digital systems and networks |
| Series H | Audiovisual and multimedia systems |
| Series I | Integrated services digital network |
| Series J | Cable networks and transmission of television, sound programme and other multimedia signals |
| Series K | Protection against interference |
| Series L | Construction, installation and protection of cables and other elements of outside plant |
| Series M | TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits |
| Series N | Maintenance: international sound programme and television transmission circuits |
| Series O | Specifications of measuring equipment |
| Series P | Telephone transmission quality, telephone installations, local line networks |
| Series Q | Switching and signalling |
| Series R | Telegraph transmission |
| Series S | Telegraph services terminal equipment |
| Series T | Terminals for telematic services |
| Series U | Telegraph switching |
| Series V | Data communication over the telephone network |
| Series X | Data networks and open system communications |
| Series Y | Global information infrastructure and Internet protocol aspects |
| Series Z | Languages and general software aspects for telecommunication systems |