To: Document Holder

From: Bellcore Customer Service

Thank you for purchasing Revision 2 to GR-82-CORE, Signaling Transfer Point (STP) Generic Requirements, Issue 2 (Bellcore, December 1996). This revision completely replaces GR-82-CORE, Issue 2, Revision 1, December 1997.

Please use the following instructions to update your document, GR–82–CORE, Issue 2, Revision 1, December 1997.

<table>
<thead>
<tr>
<th>Remove from Issue 2</th>
<th>Replace with Revision 2 Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title and Copyright Pages</td>
<td>Title and Copyright Pages</td>
</tr>
<tr>
<td>Disclaimer</td>
<td>Disclaimer</td>
</tr>
<tr>
<td>Table of Contents; List of Figures;</td>
<td>Table of Contents; List of Figures; List of</td>
</tr>
<tr>
<td>List of Tables</td>
<td>Tables</td>
</tr>
<tr>
<td>Preface</td>
<td>Preface</td>
</tr>
<tr>
<td>Sections 1 through 12</td>
<td>Sections 1 through 12</td>
</tr>
<tr>
<td>Appendixes A through J</td>
<td>Appendixes A through J</td>
</tr>
<tr>
<td>References</td>
<td>References</td>
</tr>
<tr>
<td>Glossary</td>
<td>Glossary</td>
</tr>
</tbody>
</table>
Signaling Transfer Point (STP) Generic Requirements
Signaling Transfer Point (STP)
Generic Requirements
This document, Revision 2 of GR-82-CORE, Issue 2, December 1996, completely replaces:

GR-82-CORE, Issue 2, Revision 1, December 1997.

For ordering information, see the References section of this document.

This document may not be reproduced without the express written permission of Bellcore and any reproduction without written authorization is an infringement of Bellcore’s copyright.

Copyright © 1998 Bellcore.
All rights reserved.

Project funding year: 1998
GENERIC REQUIREMENTS
NOTICE OF DISCLAIMER

This Generic Requirements document (GR) is published by Bellcore to inform the industry of Bellcore’s view of proposed generic requirements on Signaling Transfer Point (STP) Generic Requirements. These generic requirements are subject to review and change, and superseding generic requirements regarding this subject may differ from this document. Bellcore reserves the right to revise this document for any reason (consistent with applicable provisions of the Telecommunications Act of 1996 and applicable FCC rules).

Bellcore specifically advises the reader that this GR does not directly or indirectly address any Year 2000 (‘‘Y2K’’) issues that might be raised by the services, systems, equipment, specifications, descriptions, or interfaces addressed or referred to herein. As an example, and not a limitation, neither this GR nor Bellcore is directly or indirectly assessing or determining whether specific services, systems, or equipment, individually or together, in their current form, or as they may be implemented, modified, or augmented in the future, will accurately process dates and date-related data within or between the twentieth and twenty-first centuries, in either direction, including elapsed time, time difference, and/or leap year calculations.

BELLCORE, AND FUNDING PARTICIPANTS IDENTIFIED IN THE PREFACE, MAKE NO REPRESENTATION OR WARRANTY, EXPRESSED OR IMPLIED, WITH RESPECT TO THE SUFFICIENCY, ACCURACY, OR UTILITY OF ANY INFORMATION OR OPINION CONTAINED HEREIN.

BELLCORE, AND FUNDING PARTICIPANTS, EXPRESSLY ADVISE THAT ANY USE OF OR RELIANCE UPON SAID INFORMATION OR OPINION IS AT THE RISK OF THE USER AND THAT NEITHER BELLCORE, NOR ANY FUNDING PARTICIPANT, SHALL BE LIABLE FOR ANY DAMAGE OR INJURY INCURRED BY ANY PERSON ARISING OUT OF THE SUFFICIENCY, ACCURACY, OR UTILITY OF ANY INFORMATION OR OPINION CONTAINED HEREIN.

LOCAL CONDITIONS MAY GIVE RISE TO A NEED FOR ADDITIONAL PROFESSIONAL INVESTIGATIONS, MODIFICATIONS, OR SAFEGUARDS TO MEET SITE, EQUIPMENT, ENVIRONMENTAL SAFETY OR COMPANY-SPECIFIC REQUIREMENTS. IN NO EVENT IS THIS INFORMATION INTENDED TO REPLACE FEDERAL, STATE, LOCAL, OR OTHER APPLICABLE CODES, LAWS, OR REGULATIONS. SPECIFIC APPLICATIONS WILL CONTAIN VARIABLES UNKNOWN TO OR BEYOND THE CONTROL OF BELLCORE. AS A RESULT, BELLCORE CANNOT WARRANT THAT THE APPLICATION OF THIS INFORMATION WILL PRODUCE THE TECHNICAL RESULT OR SAFETY ORIGINALLY INTENDED.

This GR is not to be construed as a suggestion to anyone to modify or change any of its products or services, nor does this GR represent any commitment by anyone, including, but not limited to, Bellcore or any funder (see Preface) of this Bellcore GR to purchase, manufacture, or sell, any product with the described characteristics.
Readers are specifically advised that any entity may have needs, specifications, or requirements different from the generic descriptions herein. Therefore, anyone wishing to know any entity’s needs, specifications, or requirements should communicate directly with that entity.

Nothing contained herein shall be construed as conferring by implication, estoppel, or otherwise any license or right under any patent, whether or not the use of any information herein necessarily employs an invention of any existing or later issued patent.

Nothing contained herein is intended as a recommendation of any product to anyone.
Signaling Transfer Point (STP) Generic Requirements

Contents

Preface ................................................................................................................... Preface–1

1. Introduction ............................................................................................................... 1–1
   1.1 Purpose ............................................................................................................ 1–1
   1.2 Definitions ....................................................................................................... 1–1
   1.3 Organization of this Document ....................................................................... 1–2
   1.4 Reasons for Revision ....................................................................................... 1–3
   1.5 Related Documents ......................................................................................... 1–3
   1.6 Requirement Labeling Conventions ................................................................ 1–4
      1.6.1 Numbering of Requirement and Related Objects .............................. 1–4
      1.6.2 Requirement, Conditional Requirement, and Objective Object Identification ...................................................................................... 1–4
   1.7 Updating of this Document ............................................................................. 1–5

2. Network Architecture ................................................................................................ 2–1
   2.1 CCS Network Services .................................................................................... 2–1
      2.1.1 Circuit-Related Features .................................................................... 2–1
      2.1.2 Non-Circuit-Related Features ............................................................ 2–1
   2.2 CCS Network Components ............................................................................. 2–1
      2.2.1 CCS Switching Offices ...................................................................... 2–2
      2.2.2 Service Control Points (SCPs) ........................................................... 2–2
      2.2.3 Signaling Transfer Points (STPs) ....................................................... 2–2
      2.2.4 CCS Links .......................................................................................... 2–3
   2.3 Network Architecture ...................................................................................... 2–4
      2.3.1 Network Configurations ..................................................................... 2–4
      2.3.2 Connectivity ....................................................................................... 2–4
      2.3.3 Addressing of Signaling Points .......................................................... 2–5
         2.3.3.1 Assignment of Network Codes ................................................. 2–5
         2.3.3.2 Assignment of Cluster Codes ................................................. 2–6
         2.3.3.3 Assignment of Member Codes .............................................. 2–6

3. STP Functional Architecture ..................................................................................... 3–1
   3.1 SS7 Protocol .................................................................................................... 3–1
      3.1.1 Message Transfer Part (MTP) ............................................................ 3–1
      3.1.2 Signaling Connection Control Part (SCCP) ....................................... 3–1
      3.1.3 Integrated Services Digital Network User Part (ISDNU) ................... 3–2
      3.1.4 Transaction Capabilities Application Part (TCAP) ......................... 3–2
      3.1.5 Operations, Maintenance, and Administration Part (OMAP) .......... 3–2
3.2 STP Functions ........................................................................................................ 3–2
  3.2.1 Routing Messages ......................................................................................... 3–2
  3.2.2 Specialized Routing ..................................................................................... 3–3
  3.2.3 Carrier Signaling Access .............................................................................. 3–3
  3.2.4 Priority Processing of Network Management Tasks .................................. 3–3

3.3 Interfaces ............................................................................................................... 3–4

3.4 Capacity .................................................................................................................. 3–4

4. Signaling ..................................................................................................................... 4–1
  4.1 SS7 Protocol Overview ....................................................................................... 4–2
  4.2 Message Transfer Part (MTP) ........................................................................... 4–2
    4.2.1 Signaling Data Link .................................................................................... 4–3
    4.2.2 Signaling Link Functions ........................................................................... 4–3
    4.2.3 MTP Signaling Message Handling ......................................................... 4–4
      4.2.3.1 MTP Addresses .................................................................................. 4–4
      4.2.3.2 MTP Routing Data .......................................................................... 4–6
      4.2.3.3 Signaling Link Selection .................................................................. 4–11
      4.2.3.4 Handling of Messages Indicating Presence of Circular Routing ....... 4–14
      4.2.3.5 Message Handling During Overload .............................................. 4–15
    4.2.4 MTP Network Management Functions .................................................... 4–18
      4.2.4.1 Requirements Associated with Link Statuses, Route Statuses, and Congestion Control .................................................................................................. 4–20
      4.2.4.2 Introduction to Network Management Performance Requirements .......................................................................................................................... 4–21
      4.2.4.3 Signaling Link Changeover ................................................................ 4–22
      4.2.4.4 Signaling Link Changeback ............................................................... 4–24
      4.2.4.5 Forced Rerouting .............................................................................. 4–26
      4.2.4.6 Controlled Rerouting ....................................................................... 4–26
      4.2.4.7 MTP Restart ...................................................................................... 4–27
      4.2.4.8 Management Inhibiting/Uninhibiting .............................................. 4–42
      4.2.4.9 Signaling Traffic Flow Control ........................................................... 4–43
      4.2.4.10 Signaling Link Activation, Restoration, and Deactivation, and Link Set Activation ................................................................. 4–44
      4.2.4.11 Introduction to Cluster Management ............................................ 4–46
      4.2.4.12 Transfer-Prohibited Procedure ...................................................... 4–53
      4.2.4.13 Transfer-Allowed Procedure ........................................................... 4–63
      4.2.4.14 Transfer-Restricted Procedure ....................................................... 4–70
      4.2.4.15 Signaling-Route-Set-Test Procedure .............................................. 4–80
      4.2.4.16 Transfer-Controlled Procedure ..................................................... 4–91
      4.2.4.17 Signaling-Route-Set-Congestion-Test Procedure ....................... 4–93
      4.2.4.18 Processing of MTP Network Management Tasks During Processor Overload ................................................................. 4–93
  4.2.5 Signaling Link Tests ....................................................................................... 4–96
  4.2.6 MTP Circular Route Detection ........................................................................ 4–96
4.2.6.1 Trigger for the Circular Route Detection Test.............. 4–96
4.2.6.2 Procedures for the Circular Route Detection Test............ 4–97

4.3 Signaling Connection Control Part (SCCP).......................... 4–100
4.3.1 SCCP Addressing and Routing....................................... 4–101
  4.3.1.1 Global Title Translation and Endnodes/Databases........ 4–102
  4.3.1.2 Global Title Translation Data.................................... 4–105
  4.3.1.3 SCCP Hop Counter.................................................. 4–108
  4.3.1.4 Return Cause Parameter in UDTS and XUDTS
  Messages........................................................................... 4–109
  4.3.1.5 Verification of XUDT Message Processing
  Capability......................................................................... 4–111

4.3.2 SCCP Connectionless Control......................................... 4–111
4.3.3 SCCP Management.......................................................... 4–112
  4.3.3.1 SCCP Management Procedures - Changes to
  GR-246-CORE .................................................................... 4–113
  4.3.3.2 Additional Requirements for SCCP Management......... 4–119

4.3.4 Processing of SCCP Network Management Tasks During
Processor Overload ................................................................. 4–122

4.4 Operations, Maintenance, and Administration Part (OMAP)........ 4–123

5. Operation Requirements ......................................................................... 5–1
  5.1 Overview of the Operational Environment.............................. 5–1
  5.2 STP Provisioning Requirements............................................. 5–2
  5.2.1 Generic Program Alteration.............................................. 5–2
  5.2.2 STP Recent Change and Verify (RC&V) Functions............... 5–2
  5.2.3 STP Data Description....................................................... 5–4
    5.2.3.1 Overview of Information Modeling Methodology............ 5–4
    5.2.3.2 STP Entity/Relationship Diagrams............................. 5–9
    5.2.3.3 STP Entity Data Dictionary:....................................... 5–11
    5.2.3.4 STP Relationship Data Dictionary.............................. 5–25
    5.2.3.5 STP Attribute Data Dictionary................................... 5–31
    5.2.3.6 STP Database Updates and Data Operations................. 5–42
    5.2.3.7 Integrity Constraint Specifications............................ 5–46
    5.2.3.8 User Views and Logical Data Model........................... 5–47
  5.2.4 STP Database Management Functions................................. 5–47
    5.2.4.1 Database Updates...................................................... 5–47
    5.2.4.2 Database Assembly................................................... 5–48
    5.2.4.3 STP Database Backup................................................ 5–48
    5.2.4.4 Database Restoration................................................ 5–49
    5.2.4.5 System Initialization................................................ 5–49
    5.2.4.6 System Growth......................................................... 5–49
  5.2.5 Memory Space Accounting............................................... 5–49
    5.2.5.1 Background............................................................ 5–49
    5.2.5.2 Methodology.......................................................... 5–50
    5.2.5.3 Reporting Requirements........................................... 5–53
6. STP Performance Management ................................................................. 6–1
   6.1 Introduction ....................................................................................... 6–1
   6.2 Operations System (OS) Interfaces ..................................................... 6–2
   6.3 Measured Entity Types ...................................................................... 6–3
   6.4 Measurement Requirements ............................................................. 6–4
       6.4.1 General Requirements ................................................................. 6–4
       6.4.2 System Total Measurements ....................................................... 6–5
       6.4.3 Translation Type Measurements ............................................... 6–10
       6.4.4 Link Measurements ................................................................. 6–10
       6.4.5 Processor Measurements .......................................................... 6–14
       6.4.6 Link Set Measurements ............................................................ 6–16
       6.4.7 Special Study Measurements .................................................... 6–17
       6.4.8 Equipment Unit Type ............................................................... 6–17
   6.5 Measurement Reports ................................................................. 6–18
       6.5.1 STP System Total Report ......................................................... 6–18
       6.5.2 Component Measurement Report ............................................. 6–19
       6.5.3 Service Measurement Report ................................................... 6–19
       6.5.4 Special Study Report ............................................................... 6–19
       6.5.5 Daily Maintenance Measurement Report (SEAS System) .......... 6–19
       6.5.6 Daily Maintenance Report (Remote Maintenance OS & Local Craft Terminal) ................................................................. 6–20
       6.5.7 Day to Hour Maintenance Measurement Report (SEAS System) ... 6–20
       6.5.8 Day to Hour Maintenance Report (Remote Maintenance OS & Local Craft Terminal) ................................................................. 6–20
       6.5.9 Signaling Link Marginal Performance Report .............................. 6–21
       6.5.10 Hourly Maintenance Report (SEAS System) .............................. 6–21
       6.5.11 Hourly Maintenance Report (Remote Maintenance OS & Local Craft Terminal) ................................................................. 6–21
       6.5.12 Autonomous Network Management Reports & 5 Minute Exception Reporting ................................................................. 6–22
   6.6 Event Reporting ................................................................. 6–22
       6.6.1 Event Report Content ................................................................. 6–23
       6.6.2 Event Report Types ................................................................. 6–24
       6.6.3 Trapping Capabilities ............................................................... 6–29
       6.6.4 Routing Verification Tests ......................................................... 6–30
   6.7 Control Capabilities ................................................................. 6–30
       6.7.1 Administration of Network Management Parameters .................. 6–30
       6.7.2 Administration of Special Studies ................................................ 6–31
       6.7.3 Retrieval of Maintenance Status ............................................... 6–32
       6.7.4 Signaling Link Maintenance ...................................................... 6–32
       6.7.5 Capabilities to Support MTP Restart .............................................. 6–33

7. Network Management ............................................................................. 7–1

8. System Interfaces .................................................................................... 8–1
8.1 Signaling Interfaces............................................................................... 8–1
  8.1.1 Synchronization Requirements for DS0A Interfaces.................. 8–2
    8.1.1.1 CC Redundancy Requirements.............................................. 8–2
    8.1.1.2 CC Robustness Requirements................................................. 8–2

8.2 OS Interfaces................................................................. 8–4
  8.2.1 STP/SEAS System....................................................... 8–5
  8.2.2 STP Remote Maintenance System ........................................ 8–5

8.3 Operations Work Positions ...................................................... 8–6
  8.3.1 I/O Work Positions.............................................................. 8–6
    8.3.1.1 On-Site I/O Work Positions................................................... 8–6
    8.3.1.2 Remote I/O Work Positions................................................... 8–7
    8.3.1.3 I/O Characteristics............................................................... 8–7
    8.3.1.4 Message Routing and Echoing.............................................. 8–7

8.3.2 STP Control and Display Interface ......................................... 8–8

8.4 Security of Operations Interfaces................................................ 8–9

9. Performance ................................................................................. 9–1
  9.1 Reliability...................................................................................... 9–1
    9.1.1 General Considerations.............................................................. 9–1
    9.1.2 Service (All Causes) Downtime Objectives........................... 9–1
      9.1.2.1 MTP Level................................................................. 9–2
      9.1.2.2 SCCP Level............................................................. 9–4
      9.1.2.3 ISDN-UP................................................................. 9–4
      9.1.2.4 TCAP................................................................. 9–4
    9.1.3 Hardware Downtime Requirements........................................ 9–4
      9.1.3.1 MTP Level............................................................. 9–5
    9.1.4 Summary................................................................................ 9–5

9.2 STP Transport Time .................................................................. 9–6
  9.2.1 STP Node Processing Time ..................................................... 9–7
  9.2.2 Link Output Delay ................................................................ 9–8
  9.2.3 Cross-STP Transport Time....................................................... 9–9

9.3 Accuracy .................................................................................. 9–10

10. Environmental Requirements....................................................... 10–1
  10.1 Power....................................................................................... 10–1
  10.2 Equipment................................................................................. 10–1
  10.3 Electromagnetic and Electrical Environment............................. 10–1

11. Quality....................................................................................... 11–1
  11.1 Introduction.............................................................................. 11–1
  11.2 Reliability and Quality Switching Systems Generic Requirements...... 11–1
    11.2.1 System Design and Architecture......................................... 11–2
    11.2.2 Manufacturing and Production............................................ 11–2
    11.2.3 In-Service Performance and Product Support.......................... 11–2

12. Supplier Support ........................................................................ 12–1
12.1 Documentation on Operations .......................................................... 12–1
12.2 Software Documentation ................................................................. 12–2

Appendix A: Changes for E-Links and Complex Network Architectures .......... A–1

Appendix B: STP Requirements for Toll-Free Service .................................. B–1

B.1 Introduction ...................................................................................... B–1

B.2 MTP and SCCP Message Formats for Toll-Free Service ...................... B–1

B.2.1 MTP Message Formats ............................................................... B–1

B.2.2 SCCP Message Formats ............................................................. B–3

B.2.2.1 Overview .............................................................................. B–3

B.2.2.2 Unitdata Messages the STP Receives from the SSP ...................... B–6

B.2.2.3 SCCP Information for Toll-Free Service Messages after
Global Title Translation ................................................................. B–8

B.3 Operations ....................................................................................... B–11

B.3.1 Provisioning ................................................................................. B–11

B.3.2 Administration ............................................................................. B–12

Appendix C: STP Requirements for Gateway Function ............................... C–1

C.1 Introduction ...................................................................................... C–1

C.2 Overview of the Gateway Screening Process ...................................... C–2

C.2.1 Screening Table Structure ......................................................... C–3

C.2.2 Gateway Link Set Table ............................................................. C–5

C.2.3 Pre-GTT and Post-GTT Gateway Screening .................................. C–6

C.3 Description of Gateway Screening Tables ......................................... C–6

C.3.1 MTP Screening Tables ............................................................... C–6

C.3.2 SCCP Screening Tables ............................................................. C–10

C.3.3 ISDNUP Screening Table .......................................................... C–12

C.4 Motivation for New Screening Requirements ..................................... C–13

C.4.1 SCCP Message Type Screening ................................................. C–13

C.4.2 ISDNUP Message Type Screening ............................................. C–13

C.4.3 Gateway Message Rejection Reporting Suppression ..................... C–14

C.5 Gateway Screening Requirements ................................................... C–14

C.6 Measurements .................................................................................. C–15

C.6.1 System Totals .............................................................................. C–16

C.6.2 Link Set Utilization ...................................................................... C–16

C.6.3 Screening Results Measurements .............................................. C–17

C.6.4 Maintenance Measurements ...................................................... C–18

C.7 Performance ...................................................................................... C–18

Appendix D: Cluster Routing and Management at STPs .............................. D–1

D.1 Introduction ...................................................................................... D–1

D.1.1 Cluster Routing and Management Diversity (CRMD) ....................... D–2

D.2 Applicability of Cluster Management ............................................... D–3

D.3 Status Definitions ............................................................................ D–4

D.4 Cluster Status Maintenance ............................................................. D–4
D.4.1 Additional Status Maintenance Rules for Cluster Routing and Management Diversity ......................................................... D–8
D.5 Procedures for Cluster Management at STPs ............................................ D–9
  D.5.1 Full Point Code Management ....................................................... D–9
    D.5.1.1 Sending TFx and TCx Messages ....................................... D–10
    D.5.1.2 Receiving TFx and TCx Messages ................................... D–10
    D.5.1.3 Sending RSx and RCx Messages ...................................... D–11
    D.5.1.4 Receiving RSx and RCx Messages ................................... D–12
    D.5.1.5 Actions Taken by the STP Upon Receipt of a TFx or TCx Message ................................................................. D–12
  D.5.2 Cluster Management ................................................................... D–13
    D.5.2.1 Receipt of TFx and TCx Messages ................................... D–13
    D.5.2.2 Sending or Broadcasting TFx and TCx Messages ........... D–17
    D.5.2.3 Sending Signaling-Route-Set-Test Messages ................. D–21
    D.5.2.4 Receiving Route Set Test Messages ............................... D–23
  D.5.3 Compatibility Issues ..................................................................... D–24
  D.5.4 Interaction with SS7 Congestion Control ................................. D–26
    D.5.4.1 Local Link Congestion ....................................................... D–26
    D.5.4.2 Transfer-Controlled (TFC) Messages ......................... D–26
    D.5.4.3 Signaling-Route-Set-Congestion-Test Procedures .......... D–26
  D.5.5 Interaction with MTP Restart ..................................................... D–27
  D.5.6 Interaction With the SCCP Layer .............................................. D–27
    D.5.6.1 Point Code Status Management ................................... D–28
    D.5.6.2 Subsystem Status Management ..................................... D–28
Appendix E: STP Requirements for SCCP ISNI .......................................... E–1
  E.1 Introduction ..................................................................................... E–1
  E.2 Definition of Terms ......................................................................... E–1
  E.3 Format and Coding of the SCCP ISNI Parameter .......................... E–2
  E.4 Notation .......................................................................................... E–5
  E.5 SCCP ISNI Message Routing Procedures ...................................... E–6
    E.5.1 SCCP ISNI Network Specific Procedures ............................... E–10
    E.5.2 SCCP ISNI Constrained Routing Procedures .................... E–13
    E.5.3 SCCP ISNI Identification Procedures ..................................... E–18
    E.5.4 SCCP ISNI Error Message Procedures ................................. E–21
      E.5.4.1 Procedures for Deriving the XUDTS Message ............... E–21
      E.5.4.2 SCCP ISNI Error Message Routing Procedures .......... E–23
  E.6 Examples of SCCP ISNI Parameter Coding .................................. E–26
  E.7 SCCP ISNI Operations Requirements ............................................ E–27
    E.7.1 STP Provisioning Requirements .............................................. E–27
      E.7.1.1 User’s View of SCCP ISNI Provisioning Data ............... E–27
      E.7.1.2 Estimated Number of Provisioned Data Entries ............ E–30
    E.7.1.3 Users’ View of Data Operations ...................................... E–30
    E.7.1.4 Data Base Management Functions ................................. E–31
    E.7.2 STP Performance Management ............................................... E–31
E.7.2.1 Measurement Requirements ............................................ E–32
E.7.2.2 Event Reporting............................................................... E–33
E.8 SCCP ISNI Performance Requirements .................................................. E–36

Appendix F: Translation Type Mapping Function ........................................... F–1
F.1 Introduction ..................................................................................... F–1
F.2 Definition of Terms ............................................................................. F–1
F.3 The Translation Type Mapping Function ................................................ F–2
F.3.1 Scope of Activation ..................................................................... F–2
F.3.2 SCCP UDT and XUDT Messages ................................................. F–2
F.3.3 Incoming and Outgoing Messages ................................................. F–2
F.3.4 Gateway Screening ..................................................................... F–3
F.4 STP Operations Requirements for Translation Type Mapping ................. F–3
F.4.1 STP Provisioning Requirements ..................................................... F–3
F.4.1.1 User’s View of Translation Type Mapping Provisioning Data .......... F–4
F.4.1.2 User’s View of Data Operations ................................................. F–5
F.4.1.3 Database Management Functions ............................................. F–6
F.4.2 STP Performance Management ..................................................... F–6
F.4.2.1 Measurement Requirements ..................................................... F–6
F.4.3 Event Reporting ............................................................................. F–7
F.4.3.1 Message Tracking Capability ..................................................... F–7

Appendix G: Priority Processing of Network Management (NM) Tasks in STPs..... G–1
G.1 Introduction ..................................................................................... G–1
G.2 Monitoring of NM Processor Occupancy ........................................... G–3
G.3 STP NM Task Prioritization .............................................................. G–3
G.3.1 Signaling Traffic Management (STM) Functions ................................. G–4
G.3.1.1 Changeover/Changeback Procedures ......................................... G–5
G.3.1.2 Forced/Controlled Rerouting Procedures ..................................... G–5
G.3.1.3 MTP Restart Procedures ........................................................... G–6
G.3.1.4 Link Inhibiting/Uninhibiting ....................................................... G–6
G.3.1.5 Signaling Traffic Flow Control ................................................... G–7
G.3.1.6 Ranking of STM Tasks .............................................................. G–7
G.3.2 Signaling Route Management (SRM) Functions ................................ G–8
G.3.3 Signaling Link Management (SLM) Functions ................................ G–9
G.3.4 SCCP Management Functions ..................................................... G–10
G.4 Priority Assignments for NM Tasks ................................................... G–11
G.5 NM Task Validation .......................................................................... G–11

Appendix H: Guidelines to Determine GTT Table Sizes .................................... H–1
H.1 Introduction ..................................................................................... H–1
H.2 General Assumptions ........................................................................ H–1
H.3 Worst-Case Estimates ........................................................................ H–2
H.4 Refining Worst-Case Estimates .......................................................... H–3
List of Figures

Figure 2-1. CCS Network............................................................................................ 2–7
Figure 2-2. Example of CCS Network Architecture ................................................... 2–8
Figure 2-3. Topological View of a CCS Network....................................................... 2–9
Figure 4-1. Relationship Between Far-End PC of Link Sets at STPs and
Primary PC of Multiple PC SPCS ........................................................................ 4–124
Figure 4-2. Adjacent STP View of a Multiple PC SPCS ........................................ 4–124
Figure 4-3. Example of Routing Priorities in the Presence of E-links ..................... 4–125
Figure 5-1. Entities .................................................................................................... 5–55
Figure 5-2. Relationship ............................................................................................ 5–56
Figure 5-3. Associative Entity ................................................................................... 5–56
Figure 5-4. Composite Entity .................................................................................... 5–57
Figure 5-5. Dependent Entity .................................................................................... 5–57
Figure 5-6. Subtype Entity ........................................................................................ 5–58
Figure 5-7. Multi-Source Role Entity ....................................................................... 5–59
Figure 5-8. MTP Routing Data Model ..................................................................... 5–60
Figure 5-9. SCCP Routing Data Model ................................................................... 5–61
Figure 5-10. Generalization/Abstractions for Gateway Screening ........................... 5–62
Figure 5-11. Gateway Screening Data Model .......................................................... 5–63
Figure 9-1. Access and Backbone Network .............................................................. 9–11
Figure A-1. Message Looping without the 1st Additional Rule for Preventive
TFP/TCPs ............................................................................................................ A–3
Figure A-2. Message Looping without the 2nd Additional Rule for Preventive
TFP/TCPs ............................................................................................................ A–4
Figure C-1. Interaction among Functionalities of MTP and SCCP Processing and
Gateway Screening .............................................................................................. C–19
Figure C-2. Possible Flow of MTP Screening Steps ................................................. C–20
Figure C-3. Possible Flow of Screening Steps for MTP Network Management
Messages, SCCP, SCCP Management, and ISDNUP Messages .................. C–21
Figure D-1. Model Network Configuration .............................................................. D–29
Figure D-2. Three-Level Architecture Model ........................................................... D–30
Figure E-1. SCCP ISNI Message Routing Procedures ............................................. E–9
Figure E-2. SCCP ISNI Network Specific Procedures ............................................. E–12
Figure E-3. SCCP ISNI Constrained Routing Procedures ..................................... E–17
Figure E-4. SCCP ISNI Identification Procedures .................................................. E–20
Figure E-5. SCCP ISNI Error Message Routing Procedures ................................. E–25
Figure G-1. Network Management Priority Processing Conceptual View .................. G–2
Figure I-1. Network Model 1 .................................................................................... I–6
Figure I-2. Network Model 2 .................................................................................... I–7
Figure I-3. Network Model 3 .................................................................................... I–8
Figure I-4. Network Model 4 .................................................................................... I–9
## List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 4-1</td>
<td>Example Routeset Provisioning with Cluster Routing and E-Links</td>
<td>4–9</td>
</tr>
<tr>
<td>Table 4-2</td>
<td>Network Management Procedures for which Performance Requirements Are Provided</td>
<td>4–22</td>
</tr>
<tr>
<td>Table 6-1</td>
<td>Ranges and Provisional Values for Timers</td>
<td>6–34</td>
</tr>
<tr>
<td>Table 9-1</td>
<td>Summary of MTP STP Downtime Requirements and Objectives</td>
<td>9–6</td>
</tr>
<tr>
<td>Table 9-2</td>
<td>Summary of STP Downtime Requirements and Objectives for All Causes</td>
<td>9–6</td>
</tr>
<tr>
<td>Table 9-3</td>
<td>STP Node Processing Time</td>
<td>9–8</td>
</tr>
<tr>
<td>Table 9-4</td>
<td>Link Output Delay</td>
<td>9–9</td>
</tr>
<tr>
<td>Table 9-5</td>
<td>Cross-STP Transport Time</td>
<td>9–9</td>
</tr>
<tr>
<td>Table B-1</td>
<td>MTP Message Information</td>
<td>B–2</td>
</tr>
<tr>
<td>Table B-2</td>
<td>SCCP Unitdata Message Information</td>
<td>B–4</td>
</tr>
<tr>
<td>Table B-3</td>
<td>SCCP Information for Unitdata Messages Sent by SSP to the STP</td>
<td>B–7</td>
</tr>
<tr>
<td>Table B-4</td>
<td>SCCP Information for Toll-Free Service Messages After Global Title Translation</td>
<td>B–9</td>
</tr>
<tr>
<td>Table C-1</td>
<td>Example of Allowed OPC Table</td>
<td>C–4</td>
</tr>
<tr>
<td>Table C-2</td>
<td>Example of Blocked OPC Table</td>
<td>C–4</td>
</tr>
<tr>
<td>Table D-1</td>
<td>STP Actions Upon Receipt of a TFx or TCx</td>
<td>D–12</td>
</tr>
<tr>
<td>Table D-2</td>
<td>STP Actions Upon Receipt of TFx and TCx Messages</td>
<td>D–14</td>
</tr>
<tr>
<td>Table D-3</td>
<td>STP Actions for Cluster Routing and Management Diversity</td>
<td>D–16</td>
</tr>
<tr>
<td>Table D-4</td>
<td>STP Messages Upon Receipt of Undeliverable Message</td>
<td>D–20</td>
</tr>
<tr>
<td>Table D-5</td>
<td>STP Criteria for Sending Test Messages</td>
<td>D–22</td>
</tr>
<tr>
<td>Table D-6</td>
<td>STP Actions Upon Receipt of Test Messages</td>
<td>D–23</td>
</tr>
<tr>
<td>Table E-1</td>
<td>SCCP Intermediate Signaling Network Identification Parameter</td>
<td>E–3</td>
</tr>
<tr>
<td>Table E-2</td>
<td>Example of the SCCP ISNI Parameter with CICs</td>
<td>E–26</td>
</tr>
<tr>
<td>Table E-3</td>
<td>Example of the SCCP ISNI Parameter with the Null ICN Identity</td>
<td>E–26</td>
</tr>
<tr>
<td>Table G-1</td>
<td>Guidelines for NM Task Priority Assignments at STPs</td>
<td>G–13</td>
</tr>
<tr>
<td>Table G-2</td>
<td>Validation Matrix For Lower Priority Tasks</td>
<td>G–14</td>
</tr>
<tr>
<td>Table H-1</td>
<td>Worst Case Estimates</td>
<td>H–2</td>
</tr>
<tr>
<td>Table I-1</td>
<td>Number of GTTs per Call and Relative Service Penetration</td>
<td>I–5</td>
</tr>
<tr>
<td>Table I-2</td>
<td>Traffic Mix for Messages Received at STPs on A-links from Adjacent SSPs</td>
<td>I–10</td>
</tr>
<tr>
<td>Table I-3</td>
<td>Traffic Mix for Messages Received at RSTP pair on D-links from LSTP Pairs</td>
<td>I–10</td>
</tr>
<tr>
<td>Table I-4</td>
<td>Number of Translations at a STP Adjacent to SSPs Sending TCAP Messages</td>
<td>I–11</td>
</tr>
<tr>
<td>Table I-5</td>
<td>Number of Translations at a RSTP Connected to LSTP Pair(s)</td>
<td>I–12</td>
</tr>
<tr>
<td>Table I-6</td>
<td>STP Node Processing Time</td>
<td>I–13</td>
</tr>
</tbody>
</table>
Preface

This Preface contains important information about Bellcore’s GR process in general, as well as important information about this document.

Bellcore’s GR Process

Generic Requirements documents (GRs) provide Bellcore’s view of proposed generic criteria for telecommunications equipment, systems, or services, and involve a wide variety of factors, including interoperability, network integrity, funding participant expressed needs, and other input.

Bellcore’s GR process implements Telecommunications Act of 1996 directives relative to the development of industry-wide generic requirements relating to telecommunications equipment, including integral software and customer premises equipment. Pursuant to that Act, Bellcore invites members of the industry to fund and participate in the development process for such GRs. Invitations to fund and participate are issued monthly in the Bellcore Digest of Technical Information, and posted on Bellcore’s web site at http://www.bellcore.com/DIGEST.

At the conclusion of the GR development process, Bellcore publishes the GR, which is available by subscription. The subscription price entitles the purchaser to receive that issue of the GR (GR-CORE) along with any Issues List Report (GR-ILR) and revisions, if any are released under that GR project. ILRs contain any technical issues that arise during GR development that Bellcore and the funding participants would like further industry interaction on. The ILR may present issues for discussion, with or without proposed resolutions, and may describe proposed resolutions that lead to changes to the GR. Significant changes or additional material may be released as a revision to the GR-CORE.

Bellcore may also solicit general industry nonproprietary input regarding such GR material at the time of its publication, or through a special Industry Interaction Notice appearing in the Bellcore Digest of Technical Information. While unsolicited comments are welcome, any subsequent work by Bellcore regarding such comments will depend on funding support for such GR work. Bellcore will acknowledge receipt of comments and will provide a status to the submitting company.
About GR-82-CORE

A. Funders of GR-82-CORE, Issue 2, Revision 2 are:

Ameritech Services, Inc.
Bell Atlantic Network Services, Inc.
BellSouth Telecommunications, Inc.
Southwestern Bell Telephone Company and Pacific Bell
U S WEST Communications.

B. Relative Maturity Level

Bellcore considers this GR a mature document (i.e., TR level). It is expected that as new issues are identified through supplier comments or through newly identified needs relative to this document, an Issues List Report, GR-82-ILR, will be produced and distributed to GR-82-CORE subscribers.

To Submit Comments

When submitting comments, please include the GR document number, and cite any pertinent section and requirement number. In responding to an ILR, please identify the pertinent Issue ID number. Please provide the name and address of the contact person in your company for further discussion.

Comments should be submitted by March 31, 1999.

Send comments to:

Bellcore — GR-82-CORE
Michael Mahoney
Project Manager
331 Newman Springs Road, NVC 2Z269
Red Bank, NJ 07701-5699

Phone: (732) 758-5569
FAX: (732) 758-4343
E-Mail: mmahoney@notes.cc.bellcore.com
1. Introduction

1.1 Purpose

This Generic Requirements (GR) document provides Bellcore’s view of proposed generic requirements and objectives (collectively referred to hereinafter as “requirements”) for Signaling Transfer Points (STPs). STPs are packet switches in the Common Channel Signaling (CCS) network that transfer messages from one signaling link to another at Level 3.

A Bellcore client company (Bcc) typically uses STPs to connect various Signaling Points (SPs) within its own network (intra-network) and to connect to SPs in other networks (inter-network). STPs using the Signaling System Number 7 (SS7) protocol, as defined in GR-246-CORE, *Bellcore Specification of Signalling System Number 7 (SS7)*, provide efficient transport of messages for trunk signaling and database services in a CCS network. In addition, a primary role of the STP in a CCS network is to provide overall network management functions to help ensure the prevention, detection, recovery, and supervision of CCS network failures.

These generic requirements describe the features and functionalities of STPs by defining their interaction with the SS7 protocol, signaling networks, and operations systems. This GR is intended to help provide the basis for the CCS network architecture, procedures to implement SS7 protocols, and descriptions of provisioning, administration, and operational interfaces that can facilitate operation of the Bccs CCS networks. Also included are capacity requirements and performance objectives to meet the overall reliability standards in a Bcc environment.

These requirements state STP functions independent of implementation. Specific functions to be provided at a particular STP are to be determined by market, economic, technological, and operational considerations appropriate for the specific implementation. This GR describes functions and design practices to meet reliability, performance, security, and operations requirements in a Bcc environment.

1.2 Definitions

The following definitions apply in this document:

- **Requirement** - Feature or function that, in Bellcore's view, is necessary to satisfy the needs of a Bcc. Failure to meet a requirement may cause application restrictions, result in improper functioning of the product, or hinder operations. A requirement contains the words *shall* or *must* and is flagged by the letter R in parentheses (R).

- **Objective** - Feature or function that, in Bellcore's view, is desirable and may be required by a Bcc. An objective represents a goal to be achieved. An objective may be
reclassified as a requirement in the future. An objective is flagged by the letter O in parentheses (O), and contains the words it is desirable or it is an objective.

- **Conditional Requirement** - Feature or function that, in Bellcore's view, is necessary in specific Bcc applications; thus it may be viewed as a per-Bcc option. A conditional requirement is flagged by the letters CR in parentheses (CR).

### 1.3 Organization of this Document

The outline for the STP requirements has been modeled after FR-64, *LATA Switching Systems Generic Requirements (LSSGR)*.

Section 2 describes the CCS network plan as used in a Bcc telecommunications network. Section 3 describes the architecture of the STP in terms of functions and interfaces to other systems. Signaling functions of the STP are detailed in Section 4.

Operations requirements in Section 5 include provisioning capabilities. Support for maintenance, administration, and network management tasks are stated in Section 6.

System interfaces are described in Section 8. Section 9 contains performance requirements. Requirements for physical design and the physical environment are referenced in Section 10.

Quality assurance requirements are described in Section 11. Section 12 lists specific support expected from suppliers.

Appendix A summarizes changes to the SS7 protocol for E-links and more complex network architectures. Appendix B specifies requirements for implementing Toll-Free Service\(^1\) functions in the STP. Appendix C describes requirements for the STP Gateway function. Appendix D provides Bellcore's view of the network management procedures that will be applicable when STPs use cluster routing. Appendix E states requirements for the Intermediate Signaling Network Identification (ISNI) capability. Appendix F states requirements for the translation type mapping capability. Appendix G describes the priority processing capability for network management tasks in an STP. Appendix H provides guidelines for estimating the number of entries in GTT tables required for various services. Appendix I provides GTT capacity estimates for various service penetration levels. Appendix J provides detailed operations requirements to support SCCP functions at an STP.

---

1. Local service provider charges (e.g., hotel, cellular) or presubscription charges may apply.
1.4 Reasons for Revision

This revision of GR-82-CORE, Issue 2, includes new or changed information in the following areas:

- The sending of SBR/SNR messages (Issue 13-43 in GR-82-ILR, Issue 2C)
- The addition of text regarding the screening order that should be used for the SIO, CGPA, and CDPA data (Issue 13-111 in GR-82-ILR, Issue 2C)
- An updated requirement for allowable STP message loss (Issue 13-125 in GR-82-ILR, Issue 2C)
- A clarified requirement regarding global title translations alternate routed due to congestion (Issue 13-144 in GR-82-ILR, Issue 2C)
- Modified requirements relating to priority 3 MSU discard event reporting (Issue 13-145 in GR-82-ILR, Issue 2B).

Revisions are indicated by change bars ( | ) in the right-hand margin.

1.5 Related Documents

The features and functions defined in this GR are primarily based on functionalities necessary to support the implementation of SS7 in Bcc networks. GR-246-CORE provides detailed procedures and functionalities to be used in the Bcc signaling networks. Thus, this GR relies on detailed protocol generic requirements stated in GR-246-CORE.

North American Standards for SS7 are also available through American National Standards Institute (ANSI), Committee T1 - Telecommunications. GR-246-CORE is based on and is consistent with SS7 standards defined by the T1S1.3 Technical Subcommittee of Exchange Carriers Standards Association (ECSA) for ANSI.

In addition, there are several other generic requirements that address relevant areas of STP functionalities. GR-506-CORE, LSSGR: Signaling, Section 6.1-6.4, provides functional requirements for the CCS switching offices. GR-310-CORE, SEAS™-STP Interface Specification: User Program Layer (UPL) Application Message Descriptions and Functional Requirements, provides detailed specification for the interface between the SEAS™ system and the STP. GR-778-CORE, SEAS-STP Gateway Function Interface Specification: User Program Layer (UPL) Application Message Descriptions and Functional Requirements, provides detailed specification for the interface between the SEAS system and the STP for the purpose of supporting gateway functions. GR-1245-CORE, CCS Node Generic Requirements to Support Routing Verification Tests, provides requirements for all CCS nodes, including STPs, for the support of Message Transfer Part (MTP) Routing Verification Test (MRVT) and Signaling Connection Control Part (SCCP).

SEAS is a trademark of Bellcore.
Routing Verification Test (SRVT). GR-1087-CORE, *Generic Requirements for Common Channel Signaling (CCS) Network Usage Measurement Functionality*, provides requirements for CCS usage measurements, which would be implemented at an STP, at an STP adjunct, or by allocating functionality between an STP and an adjunct. The requirements in GR-1087-CORE may be incorporated into a future issue of GR-82-CORE. These and other documents are referenced in this document, where applicable. Readers of this GR should consult the appropriate reference document directly for detailed information.

### 1.6 Requirement Labeling Conventions

As part of Bellcore’s new GR Process, proposed requirements and objectives are labeled using conventions that are explained in the following two sections.

#### 1.6.1 Numbering of Requirement and Related Objects

Each Requirement, Objective, Condition, Conditional Requirement, and Conditional Objective object is identified by both a local and an absolute number. The local number consists of the object’s document section number and its sequence number in the section (e.g., R3-1 is the first Requirement in Section 3). The local number appears in the margin to the left of the Requirement. A Requirement object’s local number may change in subsequent issues of a document if other Requirements are added to the section or deleted.

The absolute number is a permanently assigned number that will remain for the life of the Requirement; it will not change with new issues of the document. The absolute number is presented in brackets (e.g., [2]) at the beginning of the requirement text.

Neither the local nor the absolute number of a Conditional Requirement or Conditional Objective depends on the number of the related Condition(s). If there is any ambiguity about which Conditions apply, the specific Condition(s) will be referred to by number in the text of the Conditional Requirement or Conditional Objective.

References to Requirements, Objectives, or Conditions published in other Generic Requirements documents will include both the document number and the Requirement object’s absolute number. For example, R2345-12 refers to Requirement [12] in GR–2345.

#### 1.6.2 Requirement, Conditional Requirement, and Objective Object Identification

A Requirement object may have numerous elements (paragraphs, lists, tables, equations, etc.). To aid the reader in identifying each part of the requirement, an ellipsis character (...) appears in the margin to the left of all elements of the Requirement.
Tables and Figures within Requirements are identified separately from others within the document text, and do not appear in the Table of Contents. They are numbered sequentially beginning with Table 1 and Figure 1.

1.7 Updating of this Document

This document is intended to be a comprehensive and up-to-date source of generic requirements for STPs. However, generic requirements continue to evolve, as do signaling system concepts and practices. As such, this GR and all associated references are subject to revisions or reissues as customer needs and technological capabilities change. Information on changes in this issue are provided in Section 1.5. Comments on Bellcore's proposed generic requirements from any source are welcome and will be considered for future issues of this document.
2. Network Architecture

This section gives an overview of a CCS network in terms of service provided, components, and architectural issues.

The CCS network provides signaling message transfer for participating stored program switches, databases, and operator systems in the Bcc networks. It is a packet-switched communications network that allows call control messages from the Bcc voice and data networks to be transferred on separate communications paths from the voice and data connections. The CCS messages provide for transaction-based services and for call control signaling between network nodes.

2.1 CCS Network Services

In CCS, one channel can carry addressed messages to convey signaling information relating to a multiplicity of circuits. The CCS network is also used to carry user information for services and features between switching offices and databases.

2.1.1 Circuit-Related Features

The CCS network replaces inband signaling on trunks by transporting messages between switching offices. Call control actions such as trunk seizure and answer acknowledgment result from this exchange of information.

2.1.2 Non-Circuit-Related Features

The CCS network provides features by transporting queries and responses between switching offices and databases. Other features require transport of messages between switching offices, independent of circuit connections. These features are described in the Feature Specific Documents (FSDs) of the LSSGR.

2.2 CCS Network Components

The CCS network consists of nodes called SPs, interconnected by transmission links. All nodes in the network that have CCS capabilities are SPs. Nodes that serve as intermediate signaling message transport switches are called STPs. Service Control Points (SCPs) are the SPs that provide database access to support transaction-based services. Signaling links are the transmission facilities that convey the signaling messages between two SPs. Figure 2-1 shows a schematic view of the CCS network.
2.2.1 CCS Switching Offices

Switching offices that have CCS capability are SPs on the CCS network. SPs may be end offices, tandems, or Operator Services Systems (OSSs - OSS capabilities are typically placed at some of the Access Tandem (AT) switching offices). CCS switching offices can be one of two types:

- A **Common Channel Signaling Switching Office (CCSSO)** is a switch equipped with the Integrated Services Digital Network User Part (ISDNUP) of SS7 and possibly CLASS functions such as Automatic Callback or Automatic Recall; it cannot process call services information. Requests for call services information are routed to a local or regional SSP office for access to the CCS network.

- A **Service Switching Point (SSP)** is a switch equipped to halt call processing, launch an SS7 query to obtain additional information from an SCP, and then route or treat the call based on the information received in the SCP’s response. SSPs can be end offices or tandem switches. SSPs interact with databases to provide services and routing using the feature defined in TR-NWT-000533, *Database Services: Service Switching Points*. SSPs may have the CCSSO functionality and may also be OSSs for which the requirements are stated in FR-271, *Operator Services Systems Generic Requirements (OSSGR)*. SSPs interact with databases, such as SCPs, to implement special service code features.

2.2.2 Service Control Points (SCPs)

SCPs serve as nodes for applications that consist of software and related databases. The applications can be accessed by the SSPs via a CCS network. Transactions from the SSPs to an SCP application are usually in the form of a query to the SCP followed by a response back to the node.

SCPs are always connected to a pair of STPs. SCPs may operate either in mated pairs (for increased reliability) or as stand-alone units.

2.2.3 Signaling Transfer Points (STPs)

STPs are packet switches that provide CCS message routing and transport. They are stored programmed switches that use information contained in the message in conjunction with information stored in memory to route the message to the appropriate destination signaling point.

Within the CCS network structure, STPs are Local STPs (LSTPs), Regional STPs (RSTPs), or provide both functionalities.

CLASS is a service mark of Bellcore.
• LSTPs provide the message routing functions for local services such as CLASS features within their serving area, and generally pass database queries to the RSTPs. In certain cases, LSTPs can also provide local database access.

• RSTPs may provide both local call setup services and regional access to national database services (such as 800 and calling card services).

The above designations do not necessarily indicate any functional distinction at the STP.

2.2.4 CCS Links

A communication path between two adjacent SPs in the CCS network is called a link. Presently, all links are 56-kb/s digital facilities using the SS7 protocol. It is possible that in the future link speeds other than 56-kb/s will be needed for interfaces to non-Bcc carriers (see Section 6.7).

A set of links that connect the same pair of adjacent nodes is called a link set.

In routing a message from any given SP to another SP, there may be more than one signaling link set chosen to route the message. A collection of outgoing link sets from a signaling node over which message traffic to a given destination is shared, and which is part of equally desirable routes to that destination, in terms of the priority, is referred to as a combined link set.

There are six types of links in a CCS network:

• A-link (Access link): Connects a CCSSO, SSP, or SCP to an STP.

• B-link (Bridge link): Connects STP pairs of the same hierarchical level within a network (e.g., an LSTP pair to an LSTP pair).

• C-link (Cross link): Connects a mated pair of STPs to each other.

• D-link (Diagonal link): Connects an STP on one hierarchical level to another level (e.g., an LSTP to an RSTP) or an STP in one network to an STP in another network.

(Note that B and D-links are functionally equivalent.)

• E-link (Extended link): Connects a CCSSO, SCP, or SSP to an STP that does not belong to its home STP pair. (The home STP pair for a signaling end-point is defined to be that which is connected to it via A-link sets.)

• F-link (Fully associated link): Connects a signaling end point (CCSSO, SSP, or SCP) to another signaling end point (CCSSO, SSP, or SCP).

An A-, B-, C-, D-, E-, or F-link set may consist of up to 16 links.
2.3 Network Architecture

The architecture of a given CCS network is determined by geographic considerations, the number and size of SPs, the forecasted signaling traffic load, and the features to be provided via the CCS network. A given architecture can be expected to evolve as these factors change.

Possible architectures range from employing a single pair of STPs to implementing a multi-level hierarchy of STPs. However, common requirements for any CCS network architecture are that it meet performance requirements for high reliability and low delay in message transfer (e.g., see Section 9). Network architectures should be designed to achieve a high degree of survivability. An outage should not render other SPs isolated (i.e., it should be possible to route traffic around failures). Figure 2-2 shows an example of a network architecture.

2.3.1 Network Configurations

This section describes the basic network configurations used in a typical Bcc CCS network.

The requirement of high network reliability dictates that STPs be deployed in mated pairs. The concept of mates implies that a mated STP will take over the full load of a failed or inaccessible STP. This means that an STP should be able to handle double traffic to and from adjacent SPs when a mate has failed or cannot be reached from an SP because of a link set outage.

A hierarchy of STPs is desirable. First-level STPs (LSTPs) could provide CCS network access and switch messages for a set of switching offices having the same community of interests and SCPs. Higher level STPs (RSTPs) should switch messages routed from the first-level STPs and provide access to SCPs and/or switching offices. For increased survivability of the network, STPs are located and/or deployed in diverse locations. A topological view of the CCS network configuration is depicted in Figure 2-3.

2.3.2 Connectivity

Connectivity in the CCS network must ensure alternate paths in case of link and/or STP failures.

Switching offices and SCPs should have at least two diverse links to an STP configuration to meet network access reliability objectives. Furthermore, the end SPs should have links to two STPs for survivability. Thus, the minimum access configuration is a link to each of the two STPs.
Each STP must have links to other STPs to provide alternate routes to network destinations. To meet network reliability requirements, there must be three diverse paths between two STP configurations through which any two end SPs access the CCS network.

2.3.3 Addressing of Signaling Points

Each SP (SSPs, SCPs, STPs, and CCSSOs) in a CCS network is uniquely identified by a network address called a Signaling Point Code (SPC). An SPC is a 24-bit address partitioned into three fields: the network, cluster, and member identifiers. Each field is 8 bits long, giving 256 possible codes for each field. The format for an SP code is described in GR-506-CORE, Section 6.5, and in GR-246-CORE.

2.3.3.1 Assignment of Network Codes

A CCS network is defined as a set of SPs that is commonly administered, maintained, and/or controlled. A unique network code is assigned to each North American CCS network. For some small networks, the network code, in conjunction with the network cluster code, identifies the network. For a group of SPs that is not part of a signaling network but is commonly owned or administered, blocks of SPCs in the cluster member field are assigned and administered.

According to the current guidelines described in T1.111.8 of GR-246-CORE, a CCS network that will initially provide signaling for more than 75 SPs (belonging to the network) in the first year of operation and will provide signaling for 150 SPs (belonging to the network) over the first 5 years and will have 6 network elements providing STP functionality in the first year and at least 12 network elements providing STP functionality over the first 5 years is considered a large CCS network and is assigned a unique network code. Other CCS networks are assigned small network codes. A single signaling point or group of signaling points without an STP (or STP functionality) are not considered a network and are assigned a block of signaling point codes having to share a network code and network cluster codes.

The network code of 0 is not used. The network code of 255 is reserved for future use. The network codes 1, 2, 3, and 4 are reserved for small network code assignments using the network cluster field. The network code 5 is used to assign signaling point code blocks to CCS groups.

For detailed guidelines and procedures for the assignment and administration of network codes and SP blocks, refer to T1.111.8 in GR-246-CORE. GR-246-CORE reflects the most recent, stable agreements of T1 for network code assignment guidelines. (T1 and the companies supporting T1 determine, carry out, and enforce these guidelines.)
2.3.3.2 Assignment of Cluster Codes

Network address structure supports clustering network SPs. A cluster is defined as a group of SPs that share the same community of interests (e.g., region, company, geographical area, or Local Access and Transport Area [LATA]), and directly home on a mated STP pair. A cluster of SPs can be addressed as a group. Each cluster within a given network is assigned a unique cluster code. There can be a maximum of 255 SPs per cluster. The address plan allows all members in the cluster to be referred to as a single entity for the network management function.

The following general rules apply to the assignment of cluster codes in Bcc networks:

- Each STP is assigned a unique cluster code with member number coded as 0.
- A group of SPs having the same community of interest can be assigned a unique cluster code.
- Assignment of cluster codes can be based on type of SPs. For example, a group of SCPs serving a region may have a unique cluster code. However, this does not imply assignment of cluster codes based on switching office type (e.g., 1A ESS™ system).

2.3.3.3 Assignment of Member Codes

Each SP that is the source or sink for signaling messages is assigned a unique member identification. In the Bcc networks, the member code 0 is generally assigned to an STP. This ensures that STPs do not share the same cluster identifier in a given network.

---

ESS is a trademark of Lucent Technologies.
Circles connected via dashed lines to the SSP on the bottom of the figure denote non-CCS switching offices.
Figure 2-2. Example of CCS Network Architecture
Figure 2-3. Topological View of a CCS Network
3. STP Functional Architecture

Because system architecture depends on implementation decisions, and the intent of these requirements is not to constrain implementations, the STP is described in terms of functionality and compatibility. Thus, requirements are given in terms of protocol, required functions, interfaces, and capacity. Other requirements that affect architecture, such as performance, are contained in subsequent sections.

3.1 SS7 Protocol

The SS7 protocol was designed for operation with stored program control switches in telecommunications networks. Its objective is to provide highly reliable information transfer with low delay and without loss or duplication. ANSI standards for the SS7 protocol are based on the 1988 Blue Book specification of Signaling System Number 7 (SS7) for international use issued by the CCITT. The ANSI standards define how the protocol will be used in North American networks. Bellcore is working with carriers and manufacturers in the ANSI T1S1.3 Technical Subcommittee of Committee T1 - Telecommunications on extensions and refinements of these standards.

The STP shall transport signaling messages using the SS7 protocol as stated in Bellcore GR-246-CORE. GR-246-CORE is based on and is consistent with SS7 standards defined by the T1S1.3 standards working group.

The SS7 protocol is specified in terms of the following component parts.

3.1.1 Message Transfer Part (MTP)

The MTP provides reliable transfer of signaling messages between signaling nodes. MTP functions include specifying the signaling link physical characteristics, signaling error detection and recovery, basic CCS network management, and flow control.

3.1.2 Signaling Connection Control Part (SCCP)

The SCCP provides logical signaling connections within the CCS network as well as a connectionless transfer capability for signal units. Either SCCP service may require translating information in the message to the routing address used by the MTP.

SCCP management procedures allow for alternate routing in response to failures of replicated applications at SCPs.
3.1.3 Integrated Services Digital Network User Part (ISDNUP)

The ISDNUP can use the SS7 network through the services of the MTP directly or via the SCCP. The basic signaling service of the ISDNUP is to establish circuit-switched network connections, or call setup. Passalong signaling service sends the signaling information to all switching points involved in a call connection. End-to-end signaling services provide the capability to send information directly between SPs such as the endpoints of a circuit-switched connection, or any CCS network nodes.

3.1.4 Transaction Capabilities Application Part (TCAP)

The TCAP provides the ability to exchange information (e.g., translations or commands) between CCS nodes to provide services. The TCAP uses the SCCP for transport.

3.1.5 Operations, Maintenance, and Administration Part (OMAP)

As its name indicates, OMAP contains specifications of procedures supporting operations of CCS networks. OMAP also specifies the formats of messages used in these procedures. An OMAP application uses the SS7 network through the services of TCAP, SCCP and MTP. Examples of procedures specified in OMAP are MTP Routing Verification Test (MRVT) and SCCP Routing Verification Test (SRVT). OMAP also specifies a set of measurements to be provided for the MTP and SCCP functions.

3.2 STP Functions

To provide flexibility in implementations, it is recommended that the STP functions shall be implemented in a modular fashion. Three basic functions of an STP are outlined below. More detailed requirements to perform these functions are provided in Section 4. In addition, a prioritization capability is described, which is part of the routing and specialized routing functions.

3.2.1 Routing Messages

R3-1 [1] The STP shall use the MTP to transport messages among switching offices, SCPs and other STPs.

A message route refers to a succession of signaling links on which a message is transported from the originating SP to the destination SP. The message route for a given message is predetermined by the routing label, but routing does allow for the traffic to a given destination to be transported over multiple message routes. That is, two messages with
different routing labels may be transmitted over a different succession of signaling links to a given destination.

**R3-2** [2] The STP shall use the message discrimination and distribution functions of the MTP designed to deliver the message to the proper application in the STP.

**R3-3** [3] The STP shall use the signaling network management functions to control message routing in response to congestion and failure information on the local links and on the network routes.

### 3.2.2 Specialized Routing

**R3-4** [4] The STP shall use the SCCP to perform global title translations on certain types of messages. Global titles are addresses that do not explicitly contain information allowing the MTP to route the message. An example of a global title is a dialed number that must be translated to a Destination Point Code (DPC) for MTP routing, and a Subsystem Number (SSN) for delivery to the correct application at the destination SP.

In addition, procedures for routing messages that contain an SCCP Intermediate Signaling Network Identification (ISNI) parameter are included in Appendix E.

SCCP management procedures allow alternate routing to replicated applications if an application is failed or inaccessible.

### 3.2.3 Carrier Signaling Access

**R3-5** [5] A gateway function in the STP is needed for security reasons and shall be used when other SS7 signaling networks are to interconnect with the STP in accordance with the requirements in Appendix C.

### 3.2.4 Priority Processing of Network Management Tasks

**R3-6** [6] The STP shall provide the capability to prioritize its network management functions to assure that critical network management functions receive high processing priority in its network management processors. This capability shall be particularly available when network management processor overload is experienced due to the occurrence of unanticipated failure events, but may also be provided during normal processor loading conditions. A possible prioritization scheme for network management tasks is described in Appendix G.
3.3 Interfaces

R3-7 [7] The STP shall support SS7 56-kb/s links to switching offices, SCPs, and other STPs.

The STP shall support interfaces to Operations Systems (OSs) for provisioning, administration, maintenance, and network management functions as discussed in Sections 6 and 8.2.

O3-8 [8] It is an objective that, on request from a Bcc, the STP shall support interfaces to OSs other than those discussed in Sections 6 and 8.2. Such interfaces may be used by a Bcc for provisioning, administration, maintenance, or network management functions.

The STP shall support standard interfaces for on-site and remote work positions as discussed in Sections 6 and 8.3.

3.4 Capacity

Generic requirements for the STP capacity in terms of the minimum/maximum Message Signal Unit (MSU) throughput and minimum/maximum number of links are not stated because such requirements depend on the deployment decisions that will vary among Bccs. The required capacity of an STP is a function of the projected traffic load, the specific network architecture deployed, and the functions implemented in the STPs.

The decision to use CCS for certain features and services will affect the expected load on the CCS network in terms of numbers of messages and message lengths. The forecasted load will be used to determine the number of links, and the numbers and size of STPs required in the network.

The distributed nature of a desired network architecture will affect the number and sizing of STPs. The STP may be deployed to serve a Local Access and Transport Area (LATA), a Bcc, or a regional company. Factors in the decision of how many STPs and of what size to deploy include the locations of SPs, the expected load from each, and the availability and cost of diverse facility routes.

R3-9 [9] Capacity for message handling and supporting links shall allow for handling loads under failure conditions to enhance network reliability. That is, an STP shall be able to handle the mate’s full load in addition to its normal traffic load.
R3-10 [10] The link/terminal capacity of an STP, as well as memory capacity, shall be sufficient to allow E-link deployment for direct routing as well as back-up routing, without affecting the normal STP operations.

R3-11 [11] The STP shall provide the ability for the Bcc to engineer the E-link set to handle all normal traffic as well as backup traffic destined for the E-link set. The STP shall also provide the ability for the alternate route(s) to be engineered to handle all the normal traffic together with the traffic that is normally sent on the E-link set.

An assumption in capacity planning is an engineered link load of 0.4 erlang, so that if a failure occurred, an expected 0.8 erlang of traffic would be carried by a link.
4. Signaling

An STP should communicate with other nodes in the CCS network via the SS7 protocol as defined in GR-246-CORE. (Note that the term 'signaling transfer point' in GR-246-CORE refers to a node performing an MTP relay function of receiving a message on one link and routing it to another outgoing link. In this document, additional procedures for an STP to perform other protocol functions, e.g., global title translation, routing verification tests, etc., are described.) This section will refer extensively to GR-246-CORE and, to the extent possible, will attempt to avoid the repetition of protocol details. The reader is assumed to be familiar with the SS7 protocol. Only minimal overviews of the protocol features are provided.

This section has several objectives:

- Many aspects of the SS7 protocol are stated as network administrator options, are not addressed in detail, or are not addressed at all in GR-246-CORE. Some examples are the assignment of Signaling Link Selection (SLS) codes to signaling links, broadcast of TFP/TCP messages to adjacent nodes, maintenance of cluster member routing statuses for clusters towards which cluster routing is used, etc. Specific requirements applicable to the Bccs are stated.

- Performance requirements for network management procedures are not addressed in the SS7 protocol. These requirements are presented.

- Some aspects of message handling at an STP under overload are not addressed in the SS7 protocol, and hence they are considered here.

- Some features of the SS7 protocol are very complex (e.g., the MTP restart procedure). Thus, one of the objectives is to provide clarifications.

- The SS7 protocol does not address transitional issues, e.g., for the MTP restart procedure. Such issues are addressed.

- Some of the STP requirements that are closely related to the SS7 protocol, e.g., requirements for MTP routing data or setting of congestion level thresholds for links, are not considered in GR-246-CORE. These topics are discussed.

The section is organized as follows.

Section 4.1 provides a brief overview of the SS7 protocol as used by an STP.

Section 4.2 describes STP requirements for the MTP.

Section 4.3 describes STP requirements for the SCCP.

Section 4.4 describes STP requirements for the OMAP.

Terminologies used below follow the protocol specification in GR-246-CORE.
4.1 SS7 Protocol Overview

An STP should communicate with other nodes in the CCS network using the MTP, SCCP, and OMAP of the SS7 protocol as defined in GR-246-CORE.

The MTP provides basic message handling and network management procedures used by the STP. The overall function of the MTP is to serve as a transport system providing reliable transfer of signaling messages between the locations of communicating user or application functions. The term user in this context refers to any functional entity that uses the transport capability provided by the MTP.

The SCCP builds on the MTP and provides specialized routing and management functions, for example, those necessary to provide network routing to duplicated databases, as described in Section 4.3.

OMAP (Operations, Maintenance, and Administration Part) provides functions for operations, maintenance, and administration. The two OMAP capabilities presently required in STPs are the MTP Routing Verification Test (MRVT) and SCCP Routing Verification Test (SRVT), as discussed in Section 4.4.

An STP generates MTP management, SCCP management, and OMAP messages.

R4-1 [12] An STP shall use the format specified in GR-246-CORE for messages that it generates.

As discussed in Section 2.3.5.2 in T1.111.4 of GR-246-CORE, each CCS message is assigned a congestion priority by the generating User Part. The range of priorities is 0 to 3.

R4-2 [13] For messages that an STP generates, the STP shall comply with the message prioritization scheme described in Annex A of T1.111.5 of GR-246-CORE.

4.2 Message Transfer Part (MTP)

Functions of the MTP are separated into three functional levels. Levels 1 and 2 correspond to Layers 1 and 2 of the International Standards Organization (ISO) 7498, *Basic Reference Model for Open Systems Interconnection*, and Level 3 provides a subset of Layer 3 capabilities.

The Signaling Data Link Function (Level 1) defines the physical, electrical, and functional characteristics of the signaling data link.

The Signaling Link Function (Level 2) defines procedures for transferring variable length messages over a signaling link. The unit of transfer at this level is the Signal Unit (SU), delimited by flags.
Signaling Network Functions (Level 3) route the message to the correct link or higher level function and control routing in response to changes in status of CCS network components. Flow control is also a part of the network management task at this level.

Signaling Network Functions fall into two basic categories:

- **MTP Message Handling Functions** - These are functions that, at the actual transfer of a message, direct the message to the proper signaling link or higher level functions.

- **MTP Network Management Functions** - These are functions that, on the basis of predetermined data and information about the status of the signaling network, control the current message routing and the configuration of the signaling network facilities. If the status changes, they also control reconfigurations and take other actions to preserve or restore the normal message transfer capability.

The following subsections describe the MTP functionalities that are necessary at the STP:

Section 4.2.1 considers the Signaling Data Link (Level 1) Functions.

Section 4.2.2 considers the Signaling Link (Level 2) Functions.

Section 4.2.3 considers the Signaling Message Handling Functions which form one of two subsets of the Signaling Network Functions (Level 3) of MTP.

Section 4.2.4 considers the Network Management Functions which form the second subset of the Signaling Network Functions (Level 3) of MTP.

Section 4.2.5 considers Signaling Link Tests that are run for maintenance purposes and as part of the link alignment procedure.

### 4.2.1 Signaling Data Link

**R4-3** [14] An STP shall provide the Signaling Data Link (Level 1) functionality as stated in T1.111.2 of GR-246-CORE except that an STP is only required to support 56-kb/s bit rate.

GR-246-CORE refers to 56-kb/s and 64-kb/s bit rates. Presently, only 56-kb/s rates are used in the Bcc networks and, thus, Requirement R4-3 [14] does not call for 64-kb/s bit rate.

Physical interfaces between the signaling link terminal at the STP and its assigned signaling data links shall be provided as described in Section 8.1.

### 4.2.2 Signaling Link Functions

**R4-4** [15] The STP shall provide the Signaling Link (Level 2) functionality as stated in T1.111.3 of GR-246-CORE. It may be assumed that terrestrial facilities are used for the links.
Currently, the overwhelming majority of SS7 links in Bcc networks use terrestrial facilities. It is possible, however, that satellite facilities will be used in the future, and hence, Conditional Requirement **CR4-5 [16]** applies:

**CR4-5 [16]** As a per-Bcc option, the STP shall provide an option to perform error correction by the Preventive Cyclic Retransmission (PCR) method described in T1.111.3 of GR-246-CORE. This option will be used with satellite transmission facilities. If provided, the option shall be provisionable on a per-link basis.

### 4.2.3 MTP Signaling Message Handling

The MTP signaling message handling functions form a subset of MTP Signaling Network Functions (Level 3). These are functions that, at the actual transfer of a message, direct the message to the proper signaling link or higher level functions at the STP.

**R4-6 [17]** An STP shall perform the MTP signaling message handling functions as discussed in Section 2 in T1.111.4 of GR-246-CORE. The STP shall also conform to additional requirements below.

The subsections below address the features of STP message handling functionality not covered or only partially covered in GR-246-CORE. One of the features - handling of messages indicating the presence of circular routing - is not addressed in detail in GR-246-CORE, and hence it is also addressed here.

The features addressed below are:

- MTP Addresses - Capability Code, assignment of multiple PCs to an STP and assignment of multiple PCs to an SPCS (Section 4.2.3.1)
- MTP routing data (Section 4.2.3.2)
- Signaling link selection (Section 4.2.3.3)
- Handling of messages indicating the presence of circular routing (Section 4.2.3.4)
- Message handling during overload (Section 4.2.3.5).

#### 4.2.3.1 MTP Addresses

As discussed in T1.111.8 of GR-246-CORE, each node in a CCS network is assigned an MTP network address, referred to as a Point Code (PC). Each PC is a 24-bit address partitioned into three 8-bit fields: the network identification, network cluster identification, and cluster member number. PC assignments for STPs in U.S. networks are described in T1.111.4 and T1.111.8 of GR-246-CORE.
The following topics are considered in this subsection.

- **GR-246-CORE** does not explicitly consider MTP addresses other than the Point Code. In the Bcc networks, another type of address (Capability Code) is used for STPs.

- **GR-246-CORE** assumes that only one PC is assigned to a CCS node, but it is possible that a Bcc will deploy STPs to which multiple PCs are assigned. Bellcore has not considered in detail requirements for STPs with multiple PCs, but one requirement is stated after the discussion of the Capability Code.

An SPCS (Stored Program Control Switch) in Bcc networks may be assigned up to four unique PCs. A brief description of an STP’s view of an adjacent SPCS which is assigned multiple PCs is presented at the end of the subsection.

An STP in a mated pair performing global title translation (see Section 4.3 for more information on global title translation) will usually be assigned another network address in addition to the individual PC. This additional address is referred to as a Capability Code and has the same format as a PC. The Capability Code is shared by the STPs in the pair, i.e., it is the same for both STPs.

The motivation for assigning a Capability Code is that, if a pair of STPs is assigned a Capability Code, messages requiring translation at that pair can be addressed to the Capability Code rather than to individual STPs. Thus, the presence of a Capability Code relieves Signaling End Points (SEPs) or other STPs from the burden of changing the destination address in messages requiring translation when one of the STPs in the mated pair fails, i.e., when a failure occurs, the mate will continue to perform translations and no action will be required at SEPs or STPs to address messages requiring translation to the available STP.

The Capability Code (sometimes referred to as an alias PC) may be used for functions other than global title translation in the future.

**R4-7** [18] In addition to its individual PC, an STP performing global title translation shall be able to recognize, as a minimum, one Capability Code.

**R4-8** [19] The STP shall only use its PC (never a Capability Code) in the OPC field in the routing label of messages that it originates (including those for which it performed a global title translation).

**R4-9** [20] The STP shall only use the PC (never a Capability Code) of the destination STP in the routing label of network management messages sent by network management procedures described in Sections 4.2.4 and 4.3.3 (with the exception of the signaling route set congestion test message).

Requirement **R4-10** [21] applies to STPs that support multiple PCs as their own. Note that it does *not* require that an STP must support the assignment of multiple PCs.
R4-10  [21] STPs that support multiple PCs as their own shall conform to all applicable requirements defined in this document and in GR-246-CORE. Additional requirements that may be applicable for this STP configuration are for further study.

The following is a brief description of an STP’s view of an adjacent SPCS which is assigned multiple PCs. An SPCS that supports multiple PCs has one PC designated as the primary PC while other PCs are considered secondary. Up to three secondary PCs may be assigned to an SPCS. Although an adjacent SPCS may have up to three secondary point codes assigned, the STP should provision the primary PC of the SPCS as the far-end PC of the link set connecting the STP and SPCS. In Figure 4-1, X is designated the primary PC at the SPCS and Y and Z are secondary PCs. Thus, at STP1 and STP2, the far-end PC associated with link sets A1 and A2 is provisioned as X.

From the perspective of an STP adjacent to an SPCS which is assigned multiple PCs, the SPCS will logically appear to be another STP, since a secondary PC will not be considered the far-end PC of the link set connecting the STP and SPCS. As shown in Figure 4-2, an adjacent STP will not view X, Y and Z as a single signaling point. STP1, for example, will view A1 as the primary route to PCs X, Y and Z, with PC X at the far end of A1. The link set to a multiple PC SPCS is still considered to be an A-link set (not B or D-link set).

R4-11  [22] Some of the procedures described in this document require the STP to exchange messages with a multiple PC SPCS. For some messages sent by the STP to the multiple PC SPCS, only the primary PC of the SPCS should be used as the DPC of the message (e.g., transfer-prohibited message). For some messages received from the multiple PC SPCS, the STP should only accept those message with the primary PC as the OPC (e.g., signaling-route-set-test message). These cases are explicitly described in the appropriate sections of this document. Thus, unless otherwise noted, the STP shall be able to exchange messages with a multiple PC SPCS when either the primary or a secondary PC is used, and the STP shall treat the PCs as if they represent individual signaling points.

4.2.3.2  MTP Routing Data

MTP routing data at CCS nodes specifies the destinations towards which a node may send messages, the link sets that may be taken towards those destinations, and the relative priority among the link sets.

The SS7 protocol as described in GR-246-CORE and ANSI standards does not consider explicitly the MTP routing data in CCS nodes. Section 4.2.3.2.1 presents an overview of MTP routing data at STPs. Section 4.2.3.2.2 presents requirements for MTP routing data in STPs. Section 4.2.3.2.3 presents backup routing requirements.
4.2.3.2.1 Overview of MTP Routing Data at STPs

For convenience, the term *MTP routing table* is used to refer to the collection of MTP routing data at an STP. The use of the term *table* is not intended to imply or constrain supplier implementation of data storage at an STP.

Each entry in the MTP routing table consists of the following elements:

\[ \text{Destination} - \text{Link Set Name} - \text{Cost} \]

*Link Set Name* identifies a link set which may be used to send messages to the associated destination. A link set over which messages may be sent towards a given destination will be referred to as a *route*. The route is thus an association between a link set and destination. One link set can constitute multiple routes towards different destinations. (As indicated below, the term “route” is also used to refer to two link sets of the same priority to a particular destination, i.e., a combined link set.)

The *Destination* field specifies a destination towards which the STP may send messages. This field may contain:

- Full Point Code (or Capability Code) (i.e., network, network cluster, and network cluster member identification)
- Network Cluster Address (i.e., network and network cluster identification)

If the *Destination* field contains a full Point Code, it will be said that the STP is performing *full PC routing* towards that destination. An entry provisioned in this manner is called a *member route*. The complete collection of member routes provisioned for a given Point Code destination is called a *member route set*.

If the *Destination* field contains a network cluster address, it will be said that the STP is performing *cluster routing* towards that cluster. An entry provisioned in this manner is called a *cluster route*. The complete collection of cluster routes provisioned for a given network cluster destination is called a *cluster route set*.

*Cost* indicates the relative priority of routes. A lower cost corresponds to a higher priority route so that the highest priority route has the lowest cost. Although Section 5.2.3.5 indicates that the cost (referred to as *route_relative_cost* in Section 5) may be any integer between 0 and 99, only two route priorities (denoted by 10 and 20) were used in the past. Presently (with the introduction of E-links and more complex network architectures), three priorities and possibly more may be used.

Two link sets, but no more than two, may be assigned the same cost for a given destination. Link sets of the same cost must be of the same type, i.e., B or D. Two link sets of the same cost are referred to as a *combined* link set. At an STP, a combined link set consists of B- or D-links (not A-, C-, or E-links). The (combined) link set with the lowest cost to a destination is referred to here and in GR-246-CORE as the *normal route* to that destination (it may be thought of as a route used under “normal” circumstances, i.e., a route used in the...
absence of failures). The term normal route is also used to refer to one of the link sets in a combined link set.

4.2.3.2.2 Requirements for Provisioning MTP Routing Data

This subsection considers the STP capabilities required for provisioning routes at an STP to a particular destination. More detailed provisioning requirements are presented in Section 5.2 and Section 4.2.4.11 contains detailed requirements for Cluster Routing and Management Diversity.

Generally, the most direct route from an STP to a destination is provisioned as the normal route. From the perspective of the STP, the normal link set to an adjacent signaling end point (SEP) is either the A-link set or the E-link set. If the SEP is not adjacent, a combined B-link (or D-link) set will be the normal route. The alternate link sets to the SEP will usually be the C-link set and, if E-links are deployed and cluster routing is not used to the SEP’s cluster, the combined B-link (D-link) set to another STP pair.

Requirements R4-12 [23] and R4-13 [24] express the need for an STP to support routes of 3 priorities to a node directly connected to it as shown in Figure 4-3, which presents an example of routing priorities in the presence of E-links.

R4-12 [23] If an STP has a direct A- or E-link set to a node, it shall be possible to provision that link set as the normal route. It shall also be possible to provision a (combined) B- or D-link set or C-link set as the first alternate route, and to provision the C-link set or a (combined) B- or D-link set as the second alternate route [the former would be provisioned if the first alternate route is a (combined) B- or D-link set and the latter would be assigned if the first alternate route is the C-link set].

R4-13 [24] If an STP has a direct E-link set to a node and cluster routing is not used for other members within that nodes cluster, it shall also be possible to provision that link set as either the first or second alternate route. It shall then be possible to provision a (combined) B- or D-link set as the normal route, and the C-link set as the second or first alternate route [the former would be provisioned if the E-link set is the first alternate route and the latter if the E-link set is the second alternate route].

CR4-14 [559] If an STP has a direct E-link set to a node and cluster routing is used for other members within that node’s cluster, then the STP shall require the routes that are shared between the cluster route set and the member route set (i.e., B/D-links and C-links) to be the same priority in each route set and be a higher priority than the routes that are exclusive to the member route set (i.e., the E-links).
Requirement CR4-14 [559] specifies that if cluster routing is used for a cluster that has direct link sets to members within the cluster then the direct link sets to the members must be the lowest priority routes (i.e., back-up routes) to those members. This requirement allows CRMD to function without interfering with network management. Table 4-1 provides a conceptual example of how cluster routing and full point code routing to members within the cluster should be provisioned according to CR4-14 [559].

Table 4-1. Example Routeset Provisioning with Cluster Routing and E-Links

<table>
<thead>
<tr>
<th>DPC</th>
<th>Priority</th>
<th>Linkset</th>
</tr>
</thead>
<tbody>
<tr>
<td>125-023</td>
<td>10</td>
<td>D-Link</td>
</tr>
<tr>
<td>125-023</td>
<td>20</td>
<td>C-Link</td>
</tr>
<tr>
<td>125-023-001</td>
<td>10</td>
<td>D-Link</td>
</tr>
<tr>
<td>125-023-001</td>
<td>20</td>
<td>C-Link</td>
</tr>
<tr>
<td>125-023-001</td>
<td>30</td>
<td>E-Link</td>
</tr>
</tbody>
</table>

As discussed in Section 4.2.3.1, an STP may be directly connected via an A or E-link set to an SPCS which is assigned multiple PCs. For such SPCS, it shall be possible to provision routes of 3 priorities not only to the primary PC of the SPCS (recall that the primary PC is provisioned as the far end PC of the link set connecting the STP and SPCS), but also to the secondary PCs.

R4-15 [25] If an STP has a direct A- or E-link set to an SPCS which is assigned multiple PCs, Requirements R4-12 [23] and R4-13 [24] shall apply both to the primary PC and secondary PCs of the SPCS.

Requirement R4-16 [26] expresses the need for an STP to support routes of three priorities to an adjacent (i.e., directly connected via a link set) STP that is not the mate of the STP being provisioned:

R4-16 [26] It shall be possible to provision the direct B- or D-link set to an adjacent STP, which is not the mate of the STP being provisioned, as the normal route, the B- or D-link set to the mate of that adjacent STP or C-link set as the first alternate route, and the C-link set or B- or D-link set to the mate of the adjacent STP as the second alternate route.

Requirement R4-17 [27] expresses the need for an STP to support routes of three priorities to a remote cluster or to a signaling point not directly connected to the STP.

R4-17 [27] It shall be possible to provision a (combined) B- or D-link set as the normal route to a remote cluster or to a signaling point not directly
connected to the STP; another (combined) B- or D-link set or C-link set as the first alternate route; it shall also be possible to provision the C-link set or another (combined) B- or D-link set as the second alternate route [the former would be provisioned if the first alternate route is a (combined) B- or D-link set and the latter if the first alternate route is the C-link set].

Conditional Requirement **CR4-18 [28]** reflects an option that may be desired by some Bccs to have the STP restrict the choice of first alternate route when three routes are provisioned for a destination.

**CR4-18 [28]** As a per-Bcc option, the STP may restrict the choice of the first alternate route to any destination to just the C-link set, i.e., if this option is selected, only the C-link set can be provisioned as the first alternate route.

Requirements **R4-19 [29]** and **R4-20 [30]** address cluster routing.

The previous model of cluster routing and management (documented in issues prior to and including TR-NWT-000082, Issue 4) limited the use of cluster routing to situations when every member of the cluster was accessible via the same route set. Thus, if an E-link was deployed to a single member of a remote cluster, cluster routing could not be performed. New requirements appeared in TA-NWT-000082, Issue 6 and later issues that support the networking of E-links and cluster routing and management. These requirements are hereinafter referred as cluster routing and management diversity requirements and they rely on a concept that allows member route sets to be provisioned for members of a cluster for which a cluster route set is also provisioned. If a member route set is provisioned, the STP is said to be performing full PC routing for that member. If a cluster route set is provisioned for a cluster, the STP is said to be performing cluster routing for the cluster, except for any members for which a member route set is provisioned.

**R4-19 [29]** It shall be possible to provision a cluster route set (i.e., cluster routing) to a particular cluster if the STP uses the same routing data for all members of the cluster that do not have a member route set provisioned.

**R4-20 [30]** When the STP is equipped with cluster routing and management diversity capability, it shall be possible to provision a member route set (i.e., full point code routing) to any member of a cluster, even if a cluster route set is also provisioned.

The rules for using a member route set when a cluster route set exists are stated in Section 4.2.4.11.

For more information on cluster routing see Appendix D.
4.2.3.2 Backup Routing Procedures

Requirements **R4-21** [31] and **R4-22** [32] address the procedures necessary for backup routing at an STP.

**R4-21** [31] The STP shall update the status of an affected signaling route when the status of a route changes, whether that route is the current route or not.

**R4-22** [32] On the failure of a current (combined) link set, traffic shall be diverted to the next highest priority (combined) link set that is available.

4.2.3.3 Signaling Link Selection

GR-246-CORE contains requirements for load sharing of traffic over available links in a (combined) link set (in T1.111.5).

In prior issues of GR-246-CORE and issues prior to TR-NWT-000082, Issue 4 of this document, the SLS code was assumed to be five bits. However, it was expanded to eight bits by the T1S1.3 standards working group in 1992. Such expansion allows the maximum size of a B- or D-link set to be 16 links compared to the previous value of 8. (Expansion to a number greater than 16 is not currently possible since the SLC field, which is used in several network management messages, has only 4 bits.) The expansion also allows a more even traffic distribution on links in a (combined) link set, especially after link failures. For example, with the 5-bit SLS code, traffic load between links in a link set could differ in some cases by a factor of 2. With the 8-bit SLS code, traffic will differ by less than 25% in all cases.

During the transition period from the 5-bit to the 8-bit SLS code, some CCS nodes will be using only 5 bits of the SLS field and others will be using all 8 bits. Hence, the load sharing method for the 8-bit SLS code must allow nodes that use only 5 bits to achieve as even load balance on links as possible. This results in additional complexity for the 8-bit load sharing method, as described in Section 7.3 in T1.111.5 of GR-246-CORE.

In addition, during the transition period it is important that nodes not yet updated to support 8-bit SLS should not use the 3 most significant bits of the 8-bit SLS field. For example, if those 3 bits are non-zero, the message should still be routed appropriately. Also, for messages that are originated by an STP not yet updated to support 8-bit SLS, these three bits should be “000” (as indicated by Section 15.1.2 in T1.111.4 of GR-246-CORE). This is addressed by Requirement **R4-23** [33].

**R4-23** [33] STPs that have not been updated to support 8-bit SLS routing shall not use the 3 most significant bits of the 8-bit SLS field.

The requirements for 8-bit SLS requires many of the originating nodes in the network to be updated before the benefits of more even traffic distribution can be fully realized. However,
in some circumstances, it may be desirable to achieve the benefits of the 8-bit SLS before many of the originating nodes have been updated. For example, these benefits may be desirable on the A-link sets to SCPs or B- or D-link sets. However, the performance criteria for the SLS load sharing procedures in these two cases are very different. In the near future for the SCPs of concern, message sequencing is not critical. For B-link sets, though, the ISUP signaling messages transferred on the links do require sequencing.

To achieve the benefits of the 8-bit SLS code, an STP may convert a 5-bit SLS value in a received message to an 8-bit SLS value. Depending on the situations where the 8-bit SLS code is desired, though, different requirements are needed to provide this capability. In the case where a 5-bit SLS code is received (determined by the three most significant bits being “000”) and the 8-bit SLS code benefits are desired on the A-link sets to SCPs, the three most significant bits of the SLS code could be reassigned to three other random values. If the benefits of the 8-bit SLS code are desired on B- or D-link sets, the three most significant bits must be assigned the same value for each message received on a particular signaling link to ensure proper message sequencing. However, this transition reassignment method could result in imbalances on outgoing links from the STP depending on the mapping of the SLS codes to the outgoing links. If the SLS codes are mapped in blocks to the outgoing signaling links (e.g., neglecting the fifth bit, the even concatenated\(^1\) SLS code values 16-30 map to one link; 32-46 to another link; 48-62 to another link, and so on; the odd concatenated SLS code values 17-31 map to another link; 33-47 to another link, and so on), the SLS code bits that are generated for each incoming link must be dispersed between the other five SLS bits to avoid all messages for a set of destinations from an incoming link mapping to the same outgoing link. If the SLS codes are not mapped in blocks to the outgoing signaling links (e.g., a round-robin mapping), the three generated SLS code bits may be used as the most significant bits of the 8-bit SLS code.

The following conditional requirements specify the methods in which 5-bit SLS codes are converted to 8-bit SLS codes.

**CR4-24** [34] As a Bcc-option for received messages (including messages requiring global title translation) with the three most significant bits of the SLS code of “000,” the STP shall generate a new 8-bit SLS code in one of the following ways:

- As a Bcc-option (when message sequencing is not necessary) on an outgoing link set basis, the STP shall reassign the three most significant bits of the SLS codes of receive messages in such a manner that the reassigned bits for messages to that outgoing link set are uniformly distributed over the values “000” to “111.”

- As a Bcc-option (when message sequencing is necessary), the STP shall generate three SLS code bits based on the modulo 8 sum of the

---

1. A “concatenated SLS code” is defined as the set of bits resulting from the concatenation of the three most significant bits of an 8-bit SLS code with the four least significant bits of an 8-bit SLS code.
least three significant bits of the OPC of the incoming message and a 3-bit number assigned to the incoming link. The 3-bit incoming link number must be assigned randomly within the link sets and among the link sets.

— If odd/even concatenated SLS code values greater than 15 are mapped sequentially to outgoing links (i.e., a “block” mapping, e.g., values 16, 18, 20, ..., 30 mapped to one link), the new 8-bit SLS code shall be constructed as follows:

Received SLS code: 000X₄X₃X₂X₁X₀

New SLS code (before bit rotation): X₃Y₂X₂X₄Y₁X₁Y₀X₀

where Xᵢ is a received SLS code bit and Yᵢ is a generated SLS code bit.

— For other SLS code mappings to outgoing links (i.e., not using a block mapping), the three generated SLS code bits shall be used as the three most significant bits of the new SLS code.

The STP shall not reassign the 3 most significant bits of the SLS code for received messages that do not have “000” for the 3 most significant bits. The STP shall use the revised 8-bit SLS value to select the outgoing link.

As Conditional Requirement **CR4-24** [34] indicates, the 3-bit incoming link number used to determine the revised 8-bit SLS value must be assigned randomly. Potential methods for randomly determining the 3-bit incoming link number include:

- The use of a 3-bit number randomly assigned to the link the message is received on
- The use of an existing implementation-specific number already in use by the STP for purposes such as operations
- Adding together a 3-bit number randomly assigned to each link set the message is received on and the 3 least significant bits of the SLC of the link the message is received on.

Methods other than those listed above may also be used to determine an incoming link number that is assigned randomly within the link sets and among the link sets.

**CR4-25** [35] The STP shall contain information indicating whether adjacent end nodes connected to incoming link sets are updated to send 8-bit SLS codes and whether adjacent STPs connected to incoming link sets are using the 5-to-8 bit conversion feature. This information may be maintained statically (i.e., provisioned) or dynamically (i.e., determined based on the percentage of received messages that contain an 8-bit SLS code). If the information is maintained dynamically, the adjacent signaling points shall be considered as sending 8-bit SLS codes if greater than 70% of the
messages received on a link do not have “000” as the three most significant SLS bits. For messages received from signaling points considered as sending 8-bit SLS codes, the STP does not reassign the three most significant bits of the SLS code if they are “000.”

CR4-26  [36] As a per-Bcc option for the 5-to-8 bit SLS code conversion method described in the first bullet of conditional requirement CR4-24 [34], an STP shall allow, on a recent change basis, the 5-to-8 bit SLS conversion feature to be turned “on/off” on an outgoing link set basis. The default shall be “off.” In the case of combined link sets, the “on/off” indicator value for the 5-to-8 bit SLS conversion feature for these 2 link sets should be the same.

R4-27  [37] If an STP uses the 5-to-8 bit conversion capability described in the second bullet of conditional requirement CR4-24 [34], the STP shall allow, on a recent change basis, the 5-to-8 bit SLS conversion feature to be turned “on/off” on a node basis. The default shall be “off.”

R4-28  [38] The STP shall support link set sizes of up to 16 links per link set for any link set (A-, B-, C-, D-, and E-).

4.2.3.4 Handling of Messages Indicating Presence of Circular Routing

One additional feature of message discrimination and distribution functions (see Section 2.4 in T1.111.4 in GR-246-CORE) is not addressed in detail in GR-246-CORE and hence it is discussed here. It concerns handling of messages indicating the presence of circular routing.

As discussed in Appendix A and Section 4.2.4.12.3, introduction of E-links and more complex network architectures requires that an STP should send additional preventive TFP/TCP messages under the conditions discussed in the latter section. The purpose of such TFP/TCPs is to prevent circular routing. For a variety of reasons, e.g., message loss or STP overload, a preventive TFP/TCP may not be acted upon by an adjacent STP. To help ensure that circular routing does not occur even if a preventive TFP/TCP is not acted upon, an STP must discard messages addressed to the affected destination and received from adjacent STPs to which the preventive TFP/TCP was sent.

STP actions in checking for and discarding messages indicating the presence of circular routing constitute a message discrimination function. However, since this function is closely related to the procedure for sending preventive TFP/TCP messages, it will not be discussed in detail here but rather in Section 4.2.4.12.2 describing that procedure.
4.2.3.5 Message Handling During Overload

Under the engineered failure load (defined in Section 9.2) and without failures, the message handling functions in an STP should be able to handle the offered load. Requirements R4-29 [39], R4-30 [40], and R4-31 [41] consider STP performance when message traffic exceeds the engineered failure load.

**R4-29** [39] The throughput of the STP shall be at least the engineered failure load when the offered load is greater than or equal to the engineered failure load (at least up to twice the engineered failure load). This assumes the proportion of incoming traffic to each destination remains the same as that of the engineered failure load, all the links at the STP are available, and there are no internal failures.

**R4-30** [40] If all the links at an STP are available and the offered load is that for which the STP is engineered (for failure loading), then if the incoming traffic which will be routed over a particular outgoing link set is increased (up to at least twice the engineered failure load), the total STP throughput shall be at least the level of the engineered failure load.

**R4-31** [41] If all the links at an STP are available and the offered load is that for which the STP is engineered (for failure loading), then if the incoming traffic received on a particular incoming link set is increased arbitrarily, the total STP throughput shall be at least the level of the engineered failure load.

Situations can arise in which the signaling message handling functions at an STP cannot handle messages at the rate they are received at the STP. Such situations may result, for example from a surge of traffic (in general, or for a particular outgoing route) or from failures that reduce message handling capacity. An STP should be able to control the traffic that is destined for the overloaded resources performing message handling functions in these situations. The SS7 protocol provides some procedures that may be used to deal with such overload situations. Precise criteria for using each of these procedures in overload situations are dependent on the particular implementation, but some guidelines, objectives, and requirements can be given.

An STP’s first defense against a danger of overload of the message handling functions is to reduce the rate at which incoming messages are accepted to the rate that the message handling functions can process without overload. This may result in the invocation of the Level 2 flow control procedures (described in Section 9 of T1.111.3 in GR-246-CORE) and possibly a triggering of the transfer-controlled procedures or the signaling flow control procedures at adjacent nodes. Use of the Level 2 flow control procedure may be most suitable if there is an overload of the message handling resources associated with a particular incoming link or if there is a fairly uniform overload of message handling...
resources at the STP. It is not appropriate to use this mechanism to reduce traffic on links not affected by the surge of traffic or the capacity reduction or bottleneck in the STP.

If the flow control provided by the Level 2/Level 3 interface is not sufficient to control enough traffic and alleviate the danger of overload of the message handling resources, then level 3 may discard traffic and send TFCs, as described below. If the STP does discard messages, it is an objective that low priority messages be discarded before high priority messages.

**O4-32**  [42] Excessive traffic to a few destinations or reduced capacity to handle messages to a few destinations (e.g., failed links or reduced capacity to deliver messages to those links) should not result in the discarding of messages to other destinations or delay of messages to other destinations that exceed the requirements in Sections 9.2 and 9.3.

**R4-33**  [43] An STP shall be able to detect when the resources associated with signaling message handling are in danger of becoming overloaded. The method used to detect overload, while supplier dependent, should be such that congestion controls can be performed by the STP. This is especially important when the resource that is in danger of overload will have to generate the TFC messages. If signaling message handling congestion can occur, the message handling procedures in Section 2.3.A of T1.111.4 in GR-246-CORE apply.

Although not required, it is strongly recommended that signaling message handling congestion controls use multiple congestion thresholds, if possible, to identify when the ability of the signaling message handling function has been exceeded. Three separate thresholds, numbered 1, 2, and 3, are provided to detect the onset of internal signaling message handling congestion. Similarly, three separate thresholds, numbered 1, 2, and 3, are provided to monitor the abatement of congestion.

**O4-34**  [44] It is desirable that an STP shall be able to detect and monitor signaling message handling congestion with onset and abatement thresholds as described in Section 3.8.A.1 of T1.111.4 in GR-246-CORE.

Although not required, it is strongly recommended that signaling message handling congestion controls use multiple discard thresholds, if possible, for determining whether, under signaling message handling congestion conditions, a message should be discarded or transmitted on a specified signaling link. When a message handling resource in an STP is in danger of becoming overloaded, the STP may discard traffic based on message priority, as follows:

- Discard congestion priority 0 messages when the first internal signaling message handling congestion discard threshold is reached.
Discard congestion priority 0 and 1 messages when the second internal signaling message handling congestion discard threshold is reached.

Discard congestion priority 0 through 2 messages when the third internal signaling message handling congestion discard threshold is reached.

Discard messages of any priority when the fourth internal signaling message handling congestion discard threshold is reached.

O4-35 [45] It is desirable that an STP shall be able to determine whether a message should be discarded or transmitted through the use of discard thresholds as described in Section 3.8.A.2 of T1.111.4 in GR-246-CORE.

Signaling message handling congestion discard threshold \( n \) \((n = 1, 2, \text{or } 3)\) is placed at the same point as the signaling message handling congestion onset threshold \( n \). If it can be ensured that multiple transfer-controlled messages will not be sent from the congested STP for the same message as a result of routing the message, and that the STP will not be adversely affected by routing the message, the discard threshold \( n \) may be placed higher than the onset threshold in order to minimize message loss during internal signaling message handling congestion conditions.

Under engineered loads and without failures, the rate of message discard must be limited in accordance with the requirements in Section 9.3. Even under overload or failures, the ratio of messages discarded to messages accepted must be kept small in order for the MTP to offer a useful service to its users. At this time, no specific requirements for a discard message ratio are set for overload conditions, but if the onset threshold is exceeded, it must notify the originators of those messages through the transfer controlled procedure so that traffic accessing the STP can be reduced and message loss minimized.

R4-36 [46] In addition to discarding messages as a result of danger of message handling overload, an STP shall attempt to return a transfer-controlled (TFC) message to the originator for 1 out of \( N \) \((N <= 8)\) messages of congestion priority less than 3 that are received after the onset threshold is exceeded. \( N \) shall be determined based on the particular STP architecture. For example, if the message handling resources are associated with one incoming A-link, then fewer TFCs may need to be sent and thus \( N \) can be larger (up to 8). The congestion level indicated in the TFC message shall be 3 regarding that destination when only one level of danger of overload is used. If the option to detect 4 levels is used, the congestion status reported shall correspond to the level of the danger of overload except that congestion status 3 shall also be reported for the fourth level. The TFC message shall be sent to the OPC of the received message regarding its destination (DPC). This requirement is also applicable for messages requiring global title translation. If the translation is performed before the congestion is encountered, the SCCP routing information shall be updated, as indicated in Section 4.3.3.4.
When an STP’s message handling resources are receiving more traffic than they can handle because of a capacity reduction that is unlikely to exist at its mate (e.g., for a hardware failure that is not facility related), it may be advantageous to alternate route the traffic through the mate STP, rather than control the traffic to the affected destinations.

**R4-37** [47] An STP shall send transfer-restricted (TFR) messages via the response method (as specified in Section 4.2.4.14) when signaling message handling congestion occurs due to an internal failure (i.e., not due to received traffic volumes) and is unlikely to exist at the mate STP. The affected destinations are considered restricted by the STP until the capacity reduction no longer exists. Thus, these destinations shall be considered restricted when responding to a signaling-route-set-test message (see Section 4.2.4.15 for more information on signaling-route-set-test messages) until the capacity reduction no longer exists.

Nodes receiving these TFRs will be notified that the capacity reduction no longer exists by receiving a transfer-allowed (TFA) message in response to a signaling-route-set-restricted test message (as specified in GR-246-CORE).

### 4.2.4 MTP Network Management Functions

The MTP network management functions form a subset of MTP Signaling Network Functions (Level 3). They consist of the actions and procedures required to maintain signaling service and to restore normal signaling conditions if disruptions occur in the signaling links or at SPs. These disruptions may be in the form of complete loss of a signaling link or SP due to a failure or management-initiated action, or reduced accessibility of signaling links due to congestion.

As discussed in Section 3.1 in T1.111.4 of GR-246-CORE, MTP network management functions can be categorized as follows:

1. Signaling Traffic Management Function - it is used to divert signaling traffic from a link or route to one or more different links or routes or to reduce temporarily signaling traffic in the case of congestion at an SP. It comprises the following procedures (references to Section numbers are for this document, not GR-246-CORE):
   a. Changeover (Section 4.2.4.3)
   b. Changeback (Section 4.2.4.4)
   c. Forced rerouting (Section 4.2.4.5)
   d. Controlled rerouting (Section 4.2.4.6)
   e. MTP restart at an adjacent node (Section 4.2.4.7)
   f. Management inhibiting (Section 4.2.4.8)
g. Signaling traffic flow control (Section 4.2.4.9).

2. Signaling Link Management Function - it is used to restore failed signaling links, to activate idle (not yet aligned) links and to deactivate aligned signaling links. It comprises the following procedures (references to Section numbers are for this document, not GR-246-CORE):
   a. Signaling link activation, restoration, and deactivation (Section 4.2.4.10)
   b. Link set activation (Section 4.2.4.10)
   c. Automatic allocation of terminals to links (the STP is not required to provide such automatic allocation and hence this topic is not covered in this document).

3. Signaling Route Management Function - it is used to distribute information about the signaling network status, in order to block or unblock signaling routes. It comprises the following procedures (references to Section numbers are for this document, not GR-246-CORE):
   a. Transfer-prohibited procedure (Section 4.2.4.12)
   b. Transfer-allowed procedure (Section 4.2.4.13)
   c. Transfer-restricted procedure (Section 4.2.4.14)
   d. Signaling-route-set-test procedure (Section 4.2.4.15)
   e. Transfer-controlled procedure (Section 4.2.4.16)
   f. Signaling-route-set-congestion-test procedure (Section 4.2.4.17).

4. MTP restart - this procedure is used to restart traffic between an STP that became available and the signaling network or between an available STP and an adjacent node that became accessible (Section 4.2.4.7).

The other topics covered in this section are as follows:

Section 4.2.4.1 considers requirements associated with link statuses, route statuses, STP action upon a status change, and congestion control.

Section 4.2.4.2 is an introduction to network management performance requirements.

Section 4.2.4.11 is an introduction to cluster management requirements in Sections 4.2.4.12 through 4.2.4.15 on signaling route management.

Section 4.2.4.18 considers STP processing of MTP network management tasks during processor overload.
4.2.4.1 Requirements Associated with Link Statuses, Route Statuses, and Congestion Control

The use of an MTP network management function is triggered by a change in status of signaling link(s), route(s), or the STP itself. Possible states applicable to links and routes are discussed in Section 3 in T1.111.4 of GR-246-CORE.

**R4-38** [48] An STP shall maintain status of signaling links and routes as discussed in Section 3 in T1.111.4 of GR-246-CORE. Upon a change in status of signaling link(s), route(s), or the STP itself, the STP shall apply procedures (including the false link congestion procedures, i.e., the procedures associated with timer T1.111.4/T31 which are described in Section 3.8.2.2 in T1.111.4 of GR-246-CORE) as discussed in Sections 3 and 4 in T1.111.4 of GR-246-CORE.

Section 3.8 in T1.111.4 of GR-246-CORE describes criteria for determination of signaling link congestion status and signaling route set congestion status. It also describes the network management procedures applied upon congestion status changes.

**R4-39** [49] The STP shall implement congestion thresholds as discussed in Section 3.8 in T1.111.4 of GR-246-CORE. In the presence of signaling network congestion, the STP shall take the actions discussed in Section 3.8 in T1.111.4 of GR-246-CORE.

The following additional requirements shall apply to the STP in the area of congestion thresholds and false link congestion:

**R4-40** [50] Congestion thresholds shall be provided at the STP as system parameters, changeable by the Bcc personnel on a per-link-set basis. It shall be possible to place all congestion thresholds higher than the normally engineered transmit buffer occupancy of a signaling link.

**CR4-41** [51] As per-Bcc option, the STP shall have a minimum transmit buffer (or combined retransmit and transmit buffer) size of 420 messages if the congestion thresholds are implemented in messages and at least 12,000 octets if the congestion thresholds are implemented in octets.

**R4-42** [52] When T1.111.4/T31 (the false link congestion timer) expires for a link, an STP shall remove the link from service, send Status Indication “Out of Service” (SIOS) on the link, and run the associated automatic hardware and software diagnostics to determine if a problem can be found at this end of the link. (Note, the STP does not need to run the associated diagnostics if the architecture is such that local hardware and/or software problems would have been detected via other robust mechanisms.)
STP shall then use automatic restoration routines to attempt to restore the link to service.

**R4-43** [53] An STP removing a link from service due to the expiration of T1.111.4/T31 shall notify an Operation System (OS) that the link is Out Of Service (OOS) and shall indicate the cause (i.e., T1.111.4/T31 expiration).

The false link congestion requirements assume that sending TFCs for signaling link congestion status 1 will result in a reduction of traffic. Since the ISDNUP Initial Address Messages (IAMs) were at priority one, but have recently been changed to priority zero, the STP shall provide the following option. Similarly, this option may be needed for links to SCPs, which at this time carry mainly priority one traffic.

**R4-44** [54] The STP shall provide an administerable option on an office basis to turn off monitoring links in signaling link congestion status 1 for false link congestion. When this option is selected, T1.111.4/T31 shall be started when onset threshold 2 is exceeded in the transmit buffer and canceled when the occupancy of the transmit buffer falls below abatement threshold 2.

### 4.2.4.2 Introduction to Network Management Performance Requirements

In the remainder of Section 4.2.4, requirements will appear specifying the time constraints within which an STP must perform network management actions, e.g., perform a signaling link changeover, send a Transfer-prohibited (TFP) message, etc. These time constraints, to be referred to as Network Management Performance (NMP) requirements, are typically less than 1 second.

The purpose of NMP timing requirements is to help ensure that STPs perform network management actions rapidly enough to minimize the impact of link or signaling point failures on network traffic.

Each NMP requirement specifies a time within which the corresponding network management action should be performed assuming that a single event occurred to which an STP must respond. For example, the requirement that a signaling link changeover (see Section 4.2.4.3) should be performed within 0.3 seconds of the signaling link failure assumes that only one link failed. However, Objective **O4-45** [55] emphasizes that it is highly desirable that an STP meet the NMP timing requirements even when multiple events occur simultaneously.

**O4-45** [55] It is desirable that an STP perform all network management actions within the NMP time constraints even if the STP must respond to multiple events simultaneously.
If a large number of events have occurred within a very short time period and the STP is unable to perform all actions within the NMP time constraints, the STP should perform them as closely to the required timing as possible.

For the performance requirements stated in this section, it is assumed that the delays of network management messages in transmit or receive buffer(s) are negligible.

Table 4-2 lists the network management procedures for which performance requirements are provided.

| Table 4-2. Network Management Procedures for which Performance Requirements Are Provided |
| Changeover                  |
| Changeback                  |
| Forced Rerouting            |
| Management Link Uninhibiting|
| Transfer-Prohibited         |
| Transfer-Allowed            |
| Signaling-Route-Set-Test    |
| Transfer-Controlled         |

For several network management actions, performance requirements are not stated because a time constraint is implied in GR-246-CORE, i.e., GR-246-CORE indicates that an STP has to perform those actions within a certain timer. As Requirement R4-47 [57] indicates, these actions should be performed within plus or minus 10% of the provisioned timer value.

When an STP has to perform a network management action within a timer specified in GR-246-CORE, the STP shall perform that task within plus or minus 10% of the provisioned timer value.

4.2.4.3 Signaling Link Changeover

A signaling link changeover procedure is invoked whenever a signaling link fails or is taken out of service by management inhibiting.

The STP shall initiate and perform the signaling link changeover procedure as discussed in Section 5 in T1.111.4 of GR-246-CORE.

GR-246-CORE assumes one PC per CCS node and does not consider the possibility of an SPCS which is assigned multiple PCs (see Section
4.2.3.1). Such SPCS is required to use its primary PC as the OPC in (emergency) changeover order and acknowledgment messages. (Recall that at an STP, the primary PC of the SPCS is provisioned as the far end PC of the link set connecting the STP and SPCS.) Thus an STP shall not accept a changeover order or acknowledgment message when the OPC in the message is a secondary PC of the SPCS. In addition, when sending (emergency) changeover and acknowledgment messages to a multiple PC SPCS, the STP shall use the primary PC of the SPCS as the DPC of the messages.

The remainder of this section considers performance requirements for the changeover procedure.

When a signaling link fails, the traffic that would have been routed on the failed link is buffered until it can be sent toward the new signaling link(s). For the delay of buffered messages to be minimal, it is important that an STP participating in the changeover procedure perform it as rapidly as possible.

There are two types of the changeover procedure. In the first type, nodes at the ends of the failed link exchange (emergency) changeover order and (emergency) changeover acknowledgment messages. In the second type, referred to as the time-controlled changeover, the exchange of such messages is not possible or not desirable. The node performing the changeover simply redirects traffic to the new signaling links after a delay (T1.111.4/T1) to avoid message missequencing.

The first type of the changeover procedure can be summarized as follows. A node initiating the procedure sends an (emergency) changeover order message to the node at the far end of the failed link. The remote node responds to the (emergency) changeover order message with an (emergency) changeover acknowledgment message. Upon reception of the changeover acknowledgment, the initiator of the procedure updates the retransmission buffer (unless an emergency changeover acknowledgment is received) and redirects traffic to the new signaling link(s). If an (emergency) changeover acknowledgment is not received within T1.111.4/T2, the initiator starts traffic on the new signaling link(s) anyway. The receiver of the changeover order also updates the retransmission buffer (unless an emergency changeover order is received) and redirects traffic to the new link(s). Since in this type of the changeover procedure an STP may be the sender or receiver of an (emergency) changeover order, performance requirements are stated for both cases.

At an STP initiating the changeover procedure, i.e., an STP sending an (emergency) changeover order, there are two contributions to the overall time to perform the changeover procedure:

- Delay D1 is the time that begins when the signaling link becomes unavailable and ends when the STP sends an (emergency) changeover order to the remote node (this is referred to as “failure response time” in Section 5.5.4.1 in T1.111.6 of GR-246-CORE).
• Delay D2 is the time that begins when an (emergency) changeover acknowledgment is received and ends when traffic is started on the new signaling link(s).

R4-50 [60] At an STP initiating the changeover procedure the sum of the delays D1 and D2 shall not exceed 0.3 seconds.

Requirement R4-50 [60] supersedes a requirement in Section 5.5.4.1 in T1.111.6 of GR-246-CORE which indicates that the delay D1 should not exceed 0.5 seconds for 95% of the events under traffic load that is 30% above normal.

R4-51 [61] At an STP receiving an (emergency) changeover order message, the time between reception of the message and traffic start (for all affected destinations) on the new signaling link(s) shall not exceed 0.6 seconds.

Requirement R4-51 [61] is complementary to a requirement in Section 5.5.4.2 in T1.111.6 of GR-246-CORE which indicates that the delay in sending the changeover acknowledgment message should not exceed 0.3 seconds for 95% of the events under traffic load that is 30% above normal.

(Recall that in Requirements R4-50 [60] and R4-51 [61], it is assumed that the delays of messages in transmit or receive buffer(s) are negligible.)

For the time-controlled changeover procedure, there is no separate performance requirement since a time constraint is implied by the timer T1.111.4/T1.

4.2.4.4 Signaling Link Changeback

Signaling link changeback procedure is invoked when a signaling link is brought into service as a result of link restoration (recovery from link failure), initial signaling link activation, or management uninhibiting.

R4-52 [62] The STP shall initiate and perform the signaling link changeback procedure as discussed in Section 6 in T1.111.4 of GR-246-CORE.

R4-53 [63] GR-246-CORE assumes one PC per CCS node and does not consider the possibility of an SPCS which is assigned multiple PCs (see Section 4.2.3.1). Such SPCS is required to use its primary PC as the OPC in changeback declaration and acknowledgment messages. (Recall that at an STP, the primary PC of the SPCS is provisioned as the far end PC of the link set connecting the STP and SPCS.) Thus an STP shall not accept a changeback declaration or acknowledgment message when the OPC in the message is a secondary PC of the SPCS. In addition, when sending changeback declaration and acknowledgment messages to a multiple PC SPCS, the STP shall use the primary PC of the SPCS as the DPC of the messages.
The remainder of this section considers performance requirements for the changeback procedure.

There are two types of the changeback procedure. In the first type, referred to as the sequence control procedure, the node at which a signaling link becomes available for traffic (i.e., it was uninhibited, restored, or unblocked) sends a changeback declaration message on the link being changed back from to the node terminating the signaling link that became available. The latter node should then respond with a changeback acknowledgment message. In the second type of the procedure, referred to as the time-controlled diversion procedure, the exchange of such messages is not desirable. The node performing the changeback simply redirects traffic to the new signaling link after a delay (T1.111.4/T3) to avoid message missequencing.

In the sequence control procedure, if a changeback acknowledgment is not received within T1.111.4/T4, the changeback declaration is repeated and a new timer, T1.111.4/T5, is started. If a changeback acknowledgment is still not received within T1.111.4/T5, the changeback initiator starts traffic on the newly available signaling link. Since in this type of the changeback procedure an STP may be the sender or receiver of the changeback declaration, performance requirements are stated for both cases.

At an STP initiating the changeback procedure, i.e., an STP sending the changeback declaration(s), there are several possible contributions to the time to perform the changeback procedure:

- Delay D1 is the time that begins when a signaling link becomes available for traffic and ends when the STP sends the last changeback declaration in the first set of changeback declarations sent to remote nodes.

- Delay D2 is the time that begins when a changeback acknowledgment for the last changeback declaration is received and ends when traffic from the corresponding signaling link is started on the new signaling link.

R4-54  [64] At an STP initiating the changeback procedure, the delay D1 shall not exceed 0.8 second. The delay D2 shall not exceed 0.2 second. The overall time to perform the changeback procedure shall not exceed the sum of 0.8 second plus T1.111.4/T4 plus T1.111.4/T5.

R4-55  [65] At an STP receiving a changeback declaration, the time between reception of the message and sending a changeback acknowledgment shall not exceed 0.3 second.

(Recall that in Requirements R4-54 [64] and R4-55 [65], it is assumed that the delays of messages in transmit or receive buffer(s) are negligible.)

For the time-controlled diversion procedure, there is no separate performance requirement since a time constraint is implied by the timer T1.111.4/T3.
4.2.4.5 Forced Rerouting

A forced rerouting procedure involves the diversion of signaling traffic towards the affected destination from an unavailable route to an alternate route. The objective of the procedure is to minimize consequences of a failure by restoring routing capability to a destination as quickly as possible.

An STP performs the forced rerouting procedure when a current route to a given destination becomes unavailable because of a remote failure and the STP has to divert traffic to an alternate route. The term remote failure as used here means that a failure is reported to the STP via a TFP/TCP message. A remote failure should be distinguished from a local failure of a link set, i.e., link set outage due to unavailability of signaling links. Note that the STP performs the forced rerouting procedure only for a remote failure on a route; when a local failure occurs on a link set, the STP performs a changeover procedure.

R4-56 [66] An STP shall initiate and perform the forced rerouting procedure as described in Section 7 in T1.111.4 of GR-246-CORE.

The following performance requirement shall apply to the STP:

R4-57 [67] An STP shall perform the forced rerouting procedure within 0.3 seconds of receiving the TFP/TCP message.

4.2.4.6 Controlled Rerouting

The objective of the controlled rerouting procedure is to restore the optimal signaling routing and is used in the following two cases:

R4-58 [68] The STP shall perform the controlled rerouting procedure to divert signaling traffic for a destination from the current route back to a higher or equal priority route when the latter changes status from prohibited to allowed or restricted, or from restricted to allowed. Specifically, The STP shall invoke the controlled rerouting procedure when a TFA/TCA message is received for a higher or equal priority route marked prohibited or restricted, when a TFR/TCR message is received for a route of higher priority marked prohibited, and when a TFR/TCR is received for a route of equal priority marked prohibited and the current route is marked restricted.

R4-59 [69] When a TFR/TCR message is received for a route in a combined link set marked allowed and the status of another route in the combined link set is allowed, the STP shall perform the controlled rerouting procedure to divert traffic to the latter route. Similarly, if the state of the other route in the combined link set is restricted, the STP shall perform the controlled rerouting procedure to resume loadsharing over the combined link set.
Note that the STP performs the controlled rerouting procedure when route availability is reported to the STP via a TFR/TCR or TFA/TCA message. Controlled rerouting is not performed when a link set becomes available due to a local change in link set status; a changeback procedure is performed in the latter case.

R4-60 [70] The STP shall perform the controlled rerouting procedure as discussed in Section 8 in T1.111.4 of GR-246-CORE.

There is no separate performance requirement for the controlled rerouting procedure since a time constraint is implied by the timer T1.111.4/T6.

4.2.4.7 MTP Restart

The MTP restart procedures enable an STP that is restarting to bring a sufficient number of signaling links into the available state and to update its routing tables before user signaling traffic is restarted to it. These procedures are also used by an STP when an adjacent node becomes accessible via a direct link set. MTP restart is a network management function, and occurs at Level 3 of the MTP.

The MTP restart procedures are complex and hence considered in detail in this section. The description below covers and is consistent with the material presented in GR-246-CORE. Additional requirements in the following areas are presented:

- Interim solution for transitional period where not all nodes in the CCS networks are equipped with the MTP restart procedures
- Conditions under which a restarting STP should perform the restart procedures
- Number of signaling links to be made available during the first stage of the restart procedures (i.e., while T1.111.4/T22 is running)
- Number of TRAs that need to be received from adjacent nodes during the restart procedures (i.e., while T1.111.4/T23 is running).

This section is organized into subsections as follows: Section 4.2.4.7.1 provides a brief, high-level overview of the MTP restart procedures; Section 4.2.4.7.2 discusses transitional issues pertaining to the period of time in which not all nodes in the CCS networks are equipped with the MTP restart procedures; Section 4.2.4.7.3 contains the MTP restart requirements for a restarting STP; Section 4.2.4.7.4 contains the requirements for an STP which is adjacent to a restarting node; Section 4.2.4.7.5 contains requirements concerning the receipt of unexpected MTP restart messages; and Section 4.2.4.7.6 contains general rules to be followed with respect to the procedures.

Sections 6.6.2 and 6.7 provide generic operations requirements pertaining to the MTP restart procedures at an STP. Note that some of the operations requirements which support MTP restart have been modified since the previous issue.
4.2.4.7.1 **Overview of the MTP Restart Procedures**

The MTP restart procedures use two new messages. A traffic-restart-waiting (TRW) message is an indication to the receiving node that user signaling traffic should not be sent to the originator of the TRW message until a traffic-restart-allowed (TRA) message is received from the same node. A TRA message is an indication to the receiving node that all signaling traffic may be resumed to the originator of the message. It should be noted that user signaling traffic refers to traffic generated by users of the MTP such as the ISDNUP.

The MTP restart procedures are not only performed at a restarting STP, but also at nodes adjacent to the one which is restarting. For example, a CCSSO which is adjacent to a restarting STP will go through specific steps when first interacting with the newly accessible STP. From the perspective of the restarting STP, the procedures can be broken down into several stages. First, the restarting STP attempts to bring up, or make available, in parallel, signaling links in its link sets. As links become available, the restarting STP sends TRWs to newly accessible adjacent nodes, indicating that it is not yet ready to receive any user signaling traffic. In addition to sending TRWs to adjacent nodes, the restarting STP expects to receive network management messages from adjacent nodes. For example, the restarting STP can expect to receive a TRW from each adjacent STP. This TRW is an indication to the restarting STP that the adjacent STP also needs time to complete its portion of the restart procedures before accepting user signaling traffic. Following the receipt of a TRW from an adjacent STP, the restarting STP can expect to receive signaling route management messages, specifically TFPs, TFRs, TCPs and TCRs, indicating the routes which are not allowed (i.e., routes that are restricted or prohibited) via that adjacent STP. These signaling route management messages allow the restarting STP to update its routing information which may have become inaccurate during the period of unavailability. Also, the restarting STP expects to receive TRAs from each adjacent node indicating that they are finished with their portion of the MTP restart procedures and are ready to receive user signaling traffic. After receiving TRAs from adjacent nodes, the restarting STP will broadcast, to adjacent nodes, the status of its routes which are not allowed, sending TFPs, TFRs, TCPs and TCRs. This allows adjacent nodes to update their routing information, taking into account the newly available node. Upon completing its portion of the restart procedures, the restarting STP will indicate to adjacent nodes that it is ready to receive user signaling traffic by broadcasting TRAs.

From the perspective of an STP which is adjacent to a restarting node, when the first link of a link set to a previously inaccessible node becomes accessible, the adjacent STP will recognize that the newly accessible node is restarting. It will first send the restarting node a TRW, indicating that it needs time to complete its portion of the MTP restart procedures before it is ready to receive user signaling traffic. The adjacent STP will then inform the restarting node of the status of any signaling routes which are not allowed, sending TFPs, TFRs, TCPs and TCRs. When the adjacent STP has finished its portion of the restart procedures, it will indicate this to the restarting node by sending a TRA, and will subsequently wait for a TRA from the restarting node before sending user signaling traffic.
4.2.4.7.2 Transitional Issues

In the transitional period, where not all nodes in the CCS networks have the MTP restart procedures implemented, restarting nodes may receive user signaling traffic during restart, hindering the restart procedures. It would be helpful, in the interim, if STPs could maintain information as to which adjacent nodes are not equipped with the restart procedures. This would allow a restarting STP to first make available those links connected to adjacent nodes that have the procedures implemented before bringing up links to nodes that may send user signaling traffic immediately. In doing this, the restarting STP can avoid the immediate receipt of user signaling traffic from unequipped adjacent nodes, can bring up a portion of its links (i.e., links to those nodes that have the restart procedures) and can partially update its routing information.

This information should be kept on a temporary basis, until adjacent nodes have the procedures implemented, and should be locally provisionable by the network provider. This information will only be used by an STP which is restarting, not an STP which is adjacent to a restarting node.

O4-61 [71] Information shall be kept at all STPs as to which link sets are connected to adjacent nodes not equipped with the restart procedure. The default shall be “not equipped.” A restarting STP shall update this information dynamically, as it identifies adjacent nodes equipped with the procedures. The receipt of TRWs/TRAs from adjacent nodes shall be used as an indication that they are equipped with the procedure.

4.2.4.7.3 Requirements for a Restarting STP

R4-62 [72] An unavailable STP which is ready to resume operation by making links available and resuming the exchange of signaling traffic shall initiate the MTP restart procedures when the first link(s) becomes available at Level 3.

The primary reason for initiating the MTP restart procedure at a newly available STP is that every STP has a mate that can process all of the user signaling traffic. Upon unavailability, signaling route status information may be lost, and if it is retained, it is possible that a network failure occurred during the time of the STP’s unavailability. This would cause the newly available STP to have inaccurate routing information, and be unaware of the status of a number of signaling routes. A smaller number of user signaling messages would be lost during restart if the available mate continued to process the traffic until the restarting STP reached stability.

Nodes adjacent to the unavailable STP must recognize the unavailable state of the STP if the restart procedures are to be effective. A node recognizes that another node is unavailable when it can't be reached via any route. The unavailable STP must attempt to
ensure that adjacent nodes recognize its unavailable state by continuing to remain unavailable for a predetermined time period. This allows adjacent nodes time to receive a TFP pertaining to the unavailable STP from the unavailable STP’s mate, as well as time to recognize that the direct link set to that STP is unavailable. Remaining unavailable will increase the probability that adjacent nodes recognize the unavailable state, and consequently initiate the appropriate procedures.

R4-63 [73] The restarting STP shall not begin activating links until it can ensure that it has been unavailable for a period of at least T1.111.4/T27. Processor outage may be used for the purpose of remaining unavailable.

Having been unavailable for at least a period of T1.111.4/T27, the STP may begin the restart procedures. The first step in the procedures involves bringing signaling links into the available state in order to handle the expected signaling traffic. For the restart procedures to be effective, the restarting STP should have all links available before entering the next stages of the restart procedures. Timer T1.111.4/T22 is started at the restarting STP when the first link becomes available at Level 3. When all signaling links have been made available, the restarting STP stops timer T1.111.4/T22. It is possible that under link failure conditions, the restarting STP may never have all links available. In this case, timer T1.111.4/T22 expires, and the restarting STP continues with the next stage of the restart procedures.

R4-64 [74] Upon the expiration of T1.111.4/T27, the restarting STP shall attempt first to make available the C-links to its mate STP. If the restarting STP has information pertaining to which adjacent nodes are not equipped with the node restart procedures, as per Objective O4-61 [71], it shall then attempt to bring up the A/B/D/E-links to those adjacent nodes which are equipped with the MTP restart procedures. Emergency link alignment procedures shall be used for at least the first link in each link set to be made available. The link activation procedures are those described in GR-246-CORE. The inability to bring up C-links, or those links connected to equipped adjacent nodes, shall not preclude the restarting STP from making the remaining links available. For example, one initial alignment attempt should be performed to bring up the C-links before attempting to bring up the remaining links. The restarting STP shall start timer T1.111.4/T22 when the first signaling link becomes available at Level 3. The restarting STP shall process any TRW, TRA messages received when the first signaling link goes into the in-service state at Level 2. Any TFP, TFR, TCP, TCR messages shall also be processed.

It should be noted that a signaling link may be available at Level 3 at one end, while only in-service at Level 2 at the other end, because of independent performance of the signaling link test at either end of the link. Therefore, messages may have already been received on a link which is not yet available at Level 3, and these messages must be processed.
The restarting STP sends TRWs to adjacent nodes as they become accessible via a direct link set, indicating that it is not ready to receive user signaling traffic. Like timer T1.111.4/T22, timer T1.111.4/T26 is started when the first signaling link becomes available at Level 3, at which time the first TRW is sent to an adjacent node. The adjacent node at the remote end of the newly available link starts timer T1.111.4/T25 when this TRW is received. Timer T1.111.4/T25 is restarted at the adjacent node whenever a subsequent TRW is received from the restarting STP. The purpose of T1.111.4/T26 at the restarting STP is to prompt the restarting STP, when it expires, to send adjacent nodes another TRW. Timer T1.111.4/T26 is such that it will expire at the restarting STP before timer T1.111.4/T25 expires at the adjacent node. Subsequent TRWs will indicate to the adjacent node that the restarting node is still in the process of restarting, timer T1.111.4/T25 should be restarted, and no user signaling traffic should be sent. If T1.111.4/T25 expires at the adjacent node, user signaling traffic will be resumed to the restarting node. If the restarting STP receives a TRW from an adjacent node, it will start timer T1.111.4/T25 for that node. The restarting STP will not resume user signaling traffic to the originator of the TRW until T1.111.4/T25 expires or a TRA is received from that adjacent node. Timer T1.111.4/T25 at the restarting STP allows the adjacent node some time to finish its portion of the restart procedure before any user signaling traffic is sent.

R4-65 [75] The restarting STP shall start timer T1.111.4/T26 when the first signaling link becomes available at Level 3. When the first signaling link of a link set becomes available at Level 3, the restarting STP shall send the adjacent node a TRW, and MTP Level 3 (i.e., MTP network management traffic only) traffic shall be restarted to that adjacent node. If the restarting STP receives a TRW from an adjacent node before MTP user traffic has been restarted on that link set, the restarting STP shall start T1.111.4/T25 for that link set. The restarting STP shall start timer T1.111.4/T25 upon receipt of subsequent TRWs on that link set, and MTP user traffic shall not be restarted until either a TRA is received on that link set or T1.111.4/T25 expires for that link set. The restarting STP shall continue to process any Transfer Prohibited (TFP), Transfer Restricted (TFR), Transfer Cluster Prohibited (TCP), and Transfer Cluster Restricted (TCR) messages received.

It should be noted that MTP user traffic refers to traffic generated by users of the MTP such as the ISDNUP.

R4-66 [76] If timer T1.111.4/T26 expires, the restarting STP shall restart T1.111.4/T26 and broadcast a TRW message to adjacent nodes.

R4-67 [77] Timer T1.111.4/T22 shall be stopped when all links have been made available. If a long term failure condition exists where it is known that some particular link(s) cannot be made available at the current time, timer T1.111.4/T22 shall be stopped when the remaining signaling links have

4–31
been made available. A long term failure exists if the link cannot be made available without manual intervention. This condition may be detected through internal diagnostics, and is implementation dependent.

R4-68 [78] When timer T1.111.4/T22 is stopped or expires, the restarting STP shall start timer T1.111.4/T23. Timer T1.111.4/T23 shall be stopped when the restarting STP receives a TRA from each accessible adjacent node. The restarting STP shall continue to process any TFP, TFR, TCP, TCR messages received.

The purpose of timer T1.111.4/T23 is to limit the amount of time the restarting STP waits for TRAs from adjacent nodes.

R4-69 [79] If the restarting STP has information pertaining to which adjacent nodes are equipped with the restart procedure, as per the above objective, or if it receives an indication from adjacent nodes that they are not equipped with the node restart procedures, it shall not wait for TRAs from unequipped adjacent nodes. The restarting STP shall stop timer T1.111.4/T23 when TRAs have been received from all accessible adjacent nodes which are equipped with the restart procedures. An indication may be the receipt of MTP user traffic without the receipt of TRW/TRA messages.

R4-70 [80] When timer T1.111.4/T23 is stopped or expires, the restarting STP shall start timer T1.111.4/T24. During this time the restarting STP shall inform adjacent nodes of the status of its routes which are not allowed by broadcasting TFP and TFR messages, as well as TCP and TCR messages if cluster management is employed. If a TCR was broadcast, the restarting STP shall subsequently broadcast TFP messages for prohibited members of the affected cluster according to the x-list(s) maintained for that cluster. (Whenever TFP and TFR messages are broadcast for members of a cluster for which a TCR was sent, the TFx messages shall be the next network management messages sent to the adjacent nodes according to the requirements in Sections 4.2.4.12.4 and 4.2.4.13.2.)

R4-71 [81] When broadcasting the status of routes, network management procedures shall be employed as described in GR-246-CORE. TFP, TFR, TCP, TCR messages received from adjacent nodes before the expiry/ stoppage of timer T1.111.4/T23 shall be reflected in the broadcast of these signaling route management messages.
R4-72  [82] Preventive TFP and TCP messages shall also be sent, as specified in Section 4.2.4.12.2.

Note that the sending of preventive TFPs for normal routes is not required during MTP restart.

R4-73  [83] Timer T1.111.4/T24 shall be stopped when the broadcast of these messages is complete.

It should be noted that these broadcasted messages are sent to adjacent nodes via any available route. Thus, adjacent nodes, which may be accessible only via an indirect link set (i.e., the direct link set between the restarting STP and the adjacent node is not available), will receive route status information from the restarting STP.

The purpose of timer T1.111.4/T24 is to limit the amount of time consumed by the restarting STP when broadcasting the status of its routes which are not allowed.

R4-74  [84] If timer T1.111.4/T24 expires, the sending of preventive TFP and TCP messages shall be completed, as described in Section 4.2.4.12.2, timer T1.111.4/T26 shall be stopped, and TRA messages shall be broadcast to adjacent nodes. Outgoing user signaling traffic is resumed by signaling MTP users via the MTP-RESUME primitive. The restarting STP shall also start timer T1.111.4/T29 for those points to which it has sent a TRA message. The method for sending (e.g., broadcast, response method) any remaining TFx/TCx messages that were not sent while T1.111.4/T24 was running is implementation-specific.

R4-75  [85] When timer T1.111.4/T24 is stopped, the restarting STP shall also stop timer T1.111.4/T26, broadcast TRA messages to adjacent nodes, and resume user signaling traffic by signaling MTP users via the MTP-RESUME primitive. The restarting STP shall also start timer T1.111.4/T29 for those points to which it has sent a TRA message.

At this point, the STP has completed its portion of the restart procedures. The purpose of timer T1.111.4/T29 is to allow adjacent nodes a period in which they may send the previously restarting STP a TRA/TRW message without it being perceived as an unexpected message by the restarting STP. Refer to Section 4.2.4.7.5 of this document for a more detailed discussion of timer T1.111.4/T29 and unexpected messages.

Requirements R4-76 [86] and R4-77 [87] address events which may occur later than expected during the restart procedures. For example, it is expected that all links become available at the restarting STP while timer T1.111.4/T22 is running. Since it is possible that

---

2. Preventive TFPs (TCPs) are sent to notify adjacent STPs that messages for the affected destination should not be sent to the message sender because the route might be circular.
not all links become available at this time, some links may become available during later stages of the procedures. This would be viewed as an unexpected event.

R4-76  [86] If the first link in a previously unavailable link set becomes available while timer T1.111.4/T23 or T1.111.4/T24 is running, a TRW message shall be sent to the point at the far end of the link. The necessary signaling route management messages and a TRA shall either be sent during the restart procedures or immediately thereafter. User traffic shall either be restarted on the newly available link when timer T1.111.4/T24 stops or thereafter.

R4-77  [87] If changes in the availability of links or the reception of signaling route management messages/TRAs causes the status of a destination to change while timer T1.111.4/T24 is running, this status change shall either be reflected in the broadcast of signaling route management messages by the restarting STP, or handled outside of the restart procedures.

4.2.4.7.4 Requirements for an STP Adjacent to a Restarting Node

R4-78  [88] An STP shall recognize that a previously inaccessible node is restarting when either the first link in a direct link set is in the in-service state at Level 2 or a route other than a direct link set becomes available to that node (i.e., a TFA is received concerning the restarting node).

It should be noted that an adjacent STP may receive broadcasted messages from a restarting node via a route other than a direct link set, before the restarting node is accessible via that route (i.e., a TFA has not yet been received concerning the inaccessible node). For example, if the restarting node is an STP, the adjacent STP may receive broadcasted TFPs, TFRs, TCPs and TCRs.

R4-79  [89] The adjacent STP shall update the status of its routes upon receipt of these messages. No signaling traffic shall be sent to the restarting node via the indirect route until a TFA has been received concerning the restarting node and indirect route.

R4-80  [90] If a previously inaccessible node becomes accessible via a route other than a direct link set (i.e., a TFA is received concerning the previously inaccessible node), the adjacent STP shall resume user signaling traffic via the MTP-RESUME primitive.

R4-81  [91] It shall inform the newly accessible node of the status of its routes which are not allowed, by sending TFPs, TFRs, TCPs and TCRs to the newly accessible node.
R4-82  [92] It shall also broadcast TFAs, TFRs, TCAs and TCRs concerning the newly accessible node. If a TCA is sent or broadcast, the adjacent STP shall subsequently send or broadcast TFP and TFR messages for prohibited and restricted members of the affected cluster according to the x-list(s) maintained for that cluster. If a TCR is sent or broadcast, the restarting STP shall subsequently send or broadcast TFP messages for prohibited members of the affected cluster according to the x-list(s) maintained for that cluster.

R4-83  [93] The restart procedures at an STP which is adjacent to a restarting node shall be initiated when the first link in a direct link set to a previously inaccessible node becomes available.

It should be noted that the node restart procedures will not be initiated if the previously inaccessible node first became accessible via a route other than a direct link set. Those actions are covered by Requirement R4-83 [93].

R4-84  [94] The adjacent STP shall process any TRW, TRA messages received when the first signaling link goes into the in-service state at Level 2. Any TFP, TFR, TCP, TCR messages shall also be processed.

Again, it should be noted that a signaling link may be available at Level 3 at one end, while only in-service at Level 2 at the other end, because of independent performance of the signaling link test at either end of the signaling link. Therefore, messages may have already been received on a link which is not yet available at Level 3, and these messages must be processed.

R4-85  [95] The adjacent STP shall start timer T1.111.4/T28 when the first signaling link becomes available at Level 3, if neither a TRW nor TRA has been received from the restarting node.

R4-86  [96] If a TRW or TRA message is received from the restarting node while timer T1.111.4/T28 is running or before it is started, the adjacent STP shall start timer T1.111.4/T25. It shall stop timer T1.111.4/T28 if running.

The purpose of timer T1.111.4/T28 is to guard against the possibility that the restarting node does not have the restart procedures implemented. This timer is stopped when either a TRW or TRA is received from the restarting node. When timer T1.111.4/T28 expires, the adjacent STP shall resume user signaling traffic when it has completed its portion of the restart procedures. If a TRW or TRA is received while timer T1.111.4/T28 is running, timer T1.111.4/T28 will be stopped, and timer T1.111.4/T25 will be started. The purpose of starting T1.111.4/T25 even upon receipt of a TRA is to allow the adjacent STP time to
complete its portion of the restart procedures. The adjacent STP recognizes the fact that the previously inaccessible node is equipped with the restart procedures upon receiving a TRW or TRA. The purpose of timer T1.111.4/T25 is to hold off the sending of user signaling traffic either until its expiry, or the receipt of a TRA/TRW from the restarting node.

R4-87 [97] If a TRW message is received from the restarting node while timer T1.111.4/T25 is running, the adjacent STP shall restart timer T1.111.4/T25.

R4-88 [98] The adjacent STP shall send the restarting node a TRW message when the first link in a direct link set to the previously inaccessible, restarting node becomes available at Level 3.

R4-89 [99] The adjacent STP shall then send the restarting node TFP and TFR messages, as well as TCP and TCR messages if cluster management is employed, indicating the destinations which are not allowed via that STP.

R4-90 [100] If a TCR is sent, the adjacent STP shall subsequently send TFP messages for prohibited members of the affected cluster according to the x-list(s) maintained for that cluster. The adjacent STP shall subsequently send the restarting node a TRA, after all signaling route management messages have been transmitted.

R4-91 [101] If the adjacent STP has sent the restarting node a TRA, and a TRA has been received from the restarting node, the adjacent STP shall stop timer T1.111.4/T25 or T1.111.4/T28, whichever is running.

R4-92 [102] The adjacent STP shall restart MTP user traffic to the previously unavailable node via MTP-RESUME primitives for all newly accessible destinations.

R4-93 [103] The adjacent STP shall also broadcast TFA, TFR messages for those same newly accessible destinations, as well as TCA, TCR messages, if cluster management is employed. If a TCA was broadcast, the adjacent STP shall also broadcast TFP and TFR messages for prohibited and restricted members of the affected cluster according to the x-list(s) maintained for that cluster. If a TCR was broadcast, the adjacent STP shall subsequently broadcast TFP messages for prohibited members of the affected cluster according to the x-list(s) maintained for that cluster.

R4-94 [104] If timer T1.111.4/T28 expires and a TRA message has been sent to the restarting node, the adjacent STP shall restart MTP user traffic, via the MTP-RESUME primitive, on the link set to the restarting node. The adjacent STP shall also broadcast TFA, TFR messages for those newly
accessible destinations, as well as TCA, TCR messages if cluster management is employed. If a TCA was broadcast, the adjacent STP shall subsequently broadcast TFP and TFR messages for prohibited and restricted members of the affected cluster according to the x-list(s) maintained for that cluster. If a TCR was broadcast, the adjacent STP shall subsequently broadcast TFP messages for prohibited members of the affected cluster according to the x-list(s) maintained for that cluster.

R4-95

[105] If timer T1.111.4/T28 expires and a TRA has not yet been sent to the restarting node, the adjacent STP shall start timer T1.111.4/T25, complete the sending of TFP, TFR, TCP and TCR messages, and send the restarting node a TRA. Unless a TRW message has been received from the restarting node without a subsequent TRA message, the adjacent STP shall then stop timer T1.111.4/T25 and restart MTP user traffic, via the MTP-RESUME primitive for newly accessible nodes, on the link set to the restarting node. The adjacent STP shall also broadcast TFA, TFR messages for those newly accessible destinations, as well as TCA, TCR messages if cluster management is employed. If a TCA was broadcast, the adjacent STP shall subsequently broadcast TFP and TFR messages for prohibited and restricted members of the affected cluster according to the x-list(s) maintained for that cluster. If a TCR was sent or broadcast, the restarting STP shall subsequently send or broadcast TFP messages for prohibited members of the affected cluster according to the x-list(s) maintained for that cluster.

R4-96

[106] If timer T1.111.4/T25 expires, the adjacent STP shall restart MTP user traffic, via the MTP-RESUME primitive for newly accessible nodes, on the link set to the restarting node. The adjacent STP shall also broadcast TFA, TFR messages for those newly accessible destinations, as well as TCA, TCR messages if cluster management is employed. If the adjacent STP has not yet sent a TRA to the restarting node when timer T1.111.4/T25 expires, the adjacent STP shall complete the sending of TFP, TFR, TCP, and TCR messages, and send the restarting node a TRA before user signaling traffic is restarted. If a TCA is sent or broadcast, the adjacent STP shall subsequently send or broadcast TFP messages for prohibited and restricted members of the affected cluster according to the x-list(s) maintained for that cluster. If a TCR is sent or broadcast, the restarting STP shall subsequently send or broadcast TFP messages for prohibited members of the affected cluster according to the x-list(s) maintained for that cluster.

R4-97

[107] If the adjacent STP has not received a TRA message from the restarting node by the time it resumes sending user signaling traffic to that node, the adjacent STP shall start timer T1.111.4/T29. The purpose of
timer T1.111.4/T29 is to help ensure that if a TRA or TRW is received from the restarting node after user signaling traffic has been resumed, the message is not viewed as unexpected if received while the timer is running. Refer to Section 4.2.4.7.3 for a more detailed explanation of timer T1.111.4/T29 and unexpected messages.

4.2.4.7.5 Receipt of an Unexpected TRW/TRA Message

It is possible that an STP may receive an unexpected TRW or TRA message from an adjacent node. For example, an adjacent node could have been unavailable for such a short period of time that the STP did not recognize its unavailable state. Upon receiving a TRW from an adjacent node which was not perceived as being unavailable, the STP would view this TRW as unexpected. The STP would in turn go through the actions as specified below, starting timer T1.111.4/T29 when the sending of the signaling route management messages was complete. The purpose of this timer is to ensure that if a subsequent TRW or TRA is received from the originator of the unexpected message, the TRW or TRA is not viewed as unexpected if received while timer T1.111.4/T29 is running. This is to guard against the possibility that if the adjacent node views the STPs response as unexpected, and itself responds with additional messages, the subsequent messages are not again viewed as unexpected. Timer T1.111.4/T29 could potentially avoid a deadlock condition where adjacent nodes endlessly respond to each other’s unexpected messages. A received TRW or TRA is not considered unexpected if T22, T23, or T24 is running and a direct link is in service at Level 2 to the point from which the message was received, or if T25, T28, T29 is running for the point from which the message was received. In addition, a received TRW or TRA is not considered unexpected if received at a restarting STP during the broadcast of TRAs.

It should be noted that T1.111.4/T29 is optional at end nodes. Thus, an STP may potentially receive more than one TRA from an adjacent end node, if by chance some of the MTP restart messages from the STP to the adjacent end node are lost. If more than one TRA is received from an adjacent end node, and the extra TRAs are not considered unexpected (see above description), the extra TRAs should be ignored by the STP.

R4-98 [108] If an unexpected TRW or TRA message is received, the STP shall start timer T1.111.4/T30, send to the originator of the unexpected message a TRW message followed by the necessary TFP, TFR, TCP and TCR messages for routes which are not allowed. A TRA message shall then be sent. Timer T1.111.4/T30 shall subsequently be stopped, and timer T1.111.4/T29 started.

The purpose of T1.111.4/T30 is to limit the amount of time spent by an adjacent STP broadcasting the status of its prohibited and restricted routes in response to an unexpected message.
R4-99  [109] If timer T1.111.4/T30 expires and the STP has not yet completed the sending of TFP, TFR, TCP, TCR messages to the originator of the unexpected TRW/TRA message, a TRA message shall be sent, timer T1.111.4/T29 shall be started, and the sending of preventive TFPs and TCPs shall be completed.

4.2.4.7.6  General Rules

R4-100  [110] The STP shall not perform the restarting node procedures if the restart control parameter is set to disable at the time the procedures would have been initiated. The adjacent node portion of the MTP restart procedures shall not be affected by the restart control parameter. (This is the mtp_restart_indicator attribute, defined in Section 5.2.3.5. Also, refer to Section 6.7.5.)

R4-101  [111] GR-246-CORE assumes one PC per CCS node and does not consider the possibility of an SPCS which is assigned multiple PCs (see Section 4.2.3.1). Such an SPCS is required to use its primary PC as the OPC in TRW and TRA messages. (Recall that at an STP, the primary PC of the SPCS is provisioned as the far end PC of the link set connecting the STP and SPCS.) Thus an STP shall not accept a TRW or TRA message when the OPC in the message is a secondary PC of the SPCS. In addition, when sending TRW and TRA messages to a multiple PC SPCS, the STP shall use the primary PC of the SPCS as the DPC of the messages.

R4-102  [112] A signaling point shall be considered unavailable when all connected signaling links are unavailable for transmitting/receiving signaling traffic.

R4-103  [560] An STP shall discard a TRW/TRA message from an adjacent node that is received on a link not directly connected to that adjacent node.

R4-104  [113] When an STP restarts, it shall consider, at the beginning of the restart procedure, all signaling routes to be allowed (including cluster members on an x-list) and all signaling links to be uninhibited.

O4-105  [114] If MTP restart is used in conjunction with a procedure that recovers links in a particular order then the links shall become available according to the order and time intervals specified by the ordered scheme. As adjacent nodes become available, the restarting node will then perform restart as outlined in Section 4.2.4.7.3.
It is possible, upon restart, that a restarting STP will have inaccurate routing information due to failures in the network which occurred during the period of unavailability. The restarting node considers all signaling routes to be allowed since it will be receiving accurate routing information from adjacent STPs pertaining to prohibited and restricted routes. This information will allow the restarting node to accurately update its routing tables.

**R4-106** [115] At an adjacent STP, all routes via a restarting STP shall be considered allowed at the beginning of the MTP restart procedures.

A restarting STP will also inform adjacent nodes, as part of the MTP restart procedures, of the status of its routes which are not allowed.

It should be noted that although both a restarting STP and an adjacent STP mark their routes allowed as part of the restart procedures, those routes are not immediately considered allowed for MTP user traffic. An adjacent STP will consider a route, via an adjacent restarting node, to be allowed for MTP user traffic only when the adjacent restart procedures have been completed with respect to that restarting node (i.e., a TRA is received from the restarting node or T1.111.4/T28 or T1.111.4/T25 expire). A restarting STP shall not consider a route via an adjacent node to be allowed for MTP user traffic until the adjacent node has finished its portion of the procedure (i.e., the restarting STP has received a TRA from that node, T1.111.4/T25 has expired for that node, or the restarting STP finishes its portion of the procedure, and T1.111.4/T25 is not running for that adjacent node).

**R4-107** [116] If a signaling-route-set-test message is received at a restarting STP during the restart procedures, it shall be ignored.

Ignoring received signaling-route-set-test messages at a restarting STP should help to ensure that minimal MTP user signaling traffic is received at the restarting STP. If a signaling-route-set-test prohibited message is received, ignoring the message, even though the route may be allowed or restricted, will prevent the receipt of MTP user signaling traffic for that node, giving the restarting STP more time to finish restart before routing traffic. If a signaling-route-set-test restricted message is received, ignoring the message, even though the route may be prohibited or allowed, may or may not prevent the receipt of MTP user signaling traffic for that node, depending on the status of the affected destination at the sending node. If the route to the affected destination is prohibited at the restarting STP, and the signaling-route-set-test restricted message is ignored, the sending node may attempt to route MTP user signaling traffic via the restarting STP. In this case, the restarting STP would respond with a TFP message, and the originator would be informed of the correct status. Ignoring signaling-route-set-test messages at the restarting STP, regardless of the actual route status, is intended to relieve the restarting STP of the burden of processing received signaling-route-set-test messages.
R4-108 [117] Signaling-route-set-test messages received at an STP adjacent to a restarting signaling point while timer T1.111.4/T25 or T1.111.4/T28 is running shall be handled, but the replies consider that all signaling routes using the restarting signaling point are prohibited. More specifically, the reply should consider:

... • The route to be prohibited if the only allowed/available route uses the restarting STP

... • The route to be allowed if a primary route other than one which uses the restarting STP is allowed/available

... • The route to be restricted in all other cases.

... When timer T1.111.4/T25 or T1.111.4/T28 is stopped or expires, these signaling routes shall be considered allowed unless a TFP, TFR, TCP, or TCR message was received from the restarting signaling point while timer T1.111.4/T25 or T1.111.4/T28 was running.

R4-109 [118] While timer T1.111.4/T25 or T1.111.4/T28 is running at an adjacent STP, all traffic from local Level 4 or other signaling points destined to (or to be routed through) the adjacent restarting point shall be discarded.

R4-110 [119] When an adjacent signaling point restarts, all signaling links to the restarting point shall be marked as uninhibited.

R4-111 [120] In the case that an adjacent signaling point becomes inaccessible, but routing control initiates a successful uninhibiting, no restart procedures shall be performed on either side of the link.

Routing control initiates an uninhibiting at either end of a signaling link when it is found that a destination has become inaccessible for user signaling traffic and the link sets associated with routes to that destination contain inhibited links. Therefore, nodes are not considered to be restarting when they become available due to the uninhibiting of a link.

R4-112 [121] Message traffic shall be restarted on newly available links by using the time-controlled changeback procedure, as described in GR-246-CORE.

R4-113 [122] If a link becomes unavailable during MTP restart, after having been successfully activated during the restart, time-controlled changeover shall be performed.

R4-114 [123] If a node becomes inaccessible while timer T1.111.4/T29 is running for that node, timer T1.111.4/T29 shall be stopped for that node, and that
node shall be treated as unavailable. Note that timer T1.111.4/T29 may be running at either a restarting node or a node adjacent to a restarting node.

**R4-115** [124] If signaling traffic is received from an adjacent node while the STP is restarting (i.e., TRA messages have not been sent out), then the restarting STP shall send a response mode TFP regardless of whether the route is available in response to the messages and discard the messages. If SCCP-routed messages are received at the restarting STP, the restarting STP shall respond with a response mode TFP for the STP’s capability code. A TFA shall be sent to the adjacent node to which the TFP was sent upon completion of the MTP restart procedures.

**R4-116** [125] A message concerning a local MTP user with service indicator (SI) of 0010 shall be handled normally when received at a restarting STP. Treatments for some messages with SI = 0000 received at a restarting signaling point are specified elsewhere in the previous MTP restart requirements. Other messages with SI = 0000 shall either be treated normally or discarded when received at a restarting signaling point. More specifically, the following messages with SI=0000 shall be treated normally: TFP/TCP, TFR/TCR, TFA/TCA, TRW/TRA, changeover and changeback messages, and signaling link management messages. Signaling-route-set-test messages shall be discarded. The remaining messages with SI=0000 may either be discarded or processed normally. Messages with other values of service indicator shall either be treated normally or discarded when received at a restarting signaling point.

It should be noted that a service indicator of 0010 indicates a signaling link test message, and a service indicator of 0000 indicates a signaling network management message. The service indicator is used by the message handling function in the MTP to distribute the message to the appropriate function or user within the node.

### 4.2.4.8 Management Inhibiting/Uninhibiting

The objective of management inhibiting/uninhibiting is to allow maintenance personnel, network traffic management personnel, and STP management functions to prevent/allow MSUs from being transmitted on a particular signaling link.

**R4-117** [126] The STP shall allow inhibiting and uninhibiting of signaling links by signaling management functions as described in Section 10 in T1.111.4 of GR-246-CORE. When performing link inhibiting/uninhibiting, the STP shall take the actions indicated in that section.
R4-118  [127] GR-246-CORE assumes one PC per CCS node and does not consider a possibility of an SPCS which is assigned multiple PCs (see Section 4.2.3.1). Such SPCS is required to use its primary PC as the OPC in a management inhibit/uninhibit message. (Recall that at an STP, the primary PC of the SPCS is provisioned as the far end PC of the link set connecting the STP and SPCS.) Thus an STP shall not accept a management inhibit/uninhibit message when the OPC in the message is a secondary PC of the SPCS. In addition, when sending management inhibit/uninhibit messages to a multiple PC SPCS, the STP shall use the primary PC of the SPCS as the DPC of the messages.

The following performance requirement shall apply to an STP. Note that other performance requirements related to management inhibiting/uninhibiting are implied by timers T1.111.4/T1 and T1.111.4/T3 as discussed in the sections on changeover and changeback procedures.

R4-119  [128] When node isolation requires force uninhibit of a previously inhibited link, an STP shall be able to send a signaling link force uninhibit message within 0.3 second from the time of the event causing node isolation.

4.2.4.9 Signaling Traffic Flow Control

The purpose of the signaling traffic flow control functions is to limit signaling traffic at its source when the signaling network is not capable of transferring all signaling traffic offered by User Parts because of network failures, overload situations, or other reasons. The following cases have been identified when flow control actions may be taken at an STP:

1. Failures of signaling links or SPs that result in route set unavailability.

   To summarize the discussion in Section 11.2 in T1.111.4 of GR-246-CORE, when a route set becomes unavailable, the Message Transfer Part at an STP shall give an indication to all existing (if any) User Parts that signaling messages cannot be transferred to the affected destination. It shall also send an indication when the route set becomes available. While the route set is unavailable, each User Part at the STP should take appropriate actions to stop generation of signaling information destined to the inaccessible destination.

R4-120  [129] When a route set is unavailable, the STP shall take flow control actions as discussed in Section 11.2 in T1.111.4 of GR-246-CORE.

2. Congestion of a route set or at the STP itself.

   To summarize the discussion in Section 11.2 of GR-246-CORE, the congestion status of a route set may change as a result of either the receipt of a TFC message relating to
a particular destination, or an indication of local signaling link congestion, or due to the signaling-route-set-congestion-test procedure. When such a change occurs, the Message Transfer Part at the STP shall give an indication to the local Level 4. Each user at the STP (if any) then takes appropriate actions to stop generation of signaling messages destined to the affected destination with congestion priorities lower than the specified congestion status. Messages received from local Level 4 with congestion priorities lower than the current signaling route set congestion status are discarded by the MTP.

**R4-121** [130] When a change occurs in the congestion status of a route set, the STP shall take flow control actions as discussed in Section 11.2 in T1.111.4 of GR-246-CORE.

With respect to congestion at the STP itself, the detection of congestion onset and abatement at the STP are implementation dependent. Any resulting flow control actions shall be consistent with the procedures specified for route set congestion. See also the discussion in Section 4.2.3.5.

3. Unavailability of a local User Part.

GR-246-CORE defines unavailability of a local User Part as failure or the non-existence of a local User Part. However, presently the only User Part at an STP is the SCCP. It is assumed that the SCCP cannot become unavailable at an STP or signaling end point without the MTP becoming unavailable, and thus, the condition of a failure of a local or remote User Part is assumed not to impact the STP. GR-246-CORE also states that a UPU (User Part Unavailable) message is sent when a received message is addressed to a non-existent local MTP user. Since the MTP flow control procedures associated with the unavailability of SCCP (local and remote) are not needed at an STP in a Bcc network, it is assumed that the benefit of sending a UPU for an unequipped user or processing a received UPU message does not justify the costs associated with implementing and deploying this capability at an STP. Thus, sending a UPU for a received message addressed to a non-existent MTP user and processing a received UPU message is not required of an STP in a Bcc network. (An STP shall be able to through-switch a received UPU message as a normal message.)

**4.2.4.10 Signaling Link Activation, Restoration, and Deactivation, and Link Set Activation**

This subsection considers requirements for the Signaling Link Management function, which consists of the procedures for signaling link activation, restoration, and deactivation, and link set activation.

**R4-122** [131] The STP shall activate, restore, and deactivate signaling links as discussed in Section 12 in T1.111.4 of GR-246-CORE.
To summarize the material in GR-246-CORE, in order to activate a signaling link, the STP will attempt to align the link as described in T1.111.3 of GR-246-CORE. If initial alignment fails, new initial alignment procedures shall be started after a delay of T1.111.4/T17 seconds. Alignment attempts shall continue indefinitely, but if alignment is not achieved before T1.111.4/T19 expires, the failure to align shall be reported (and alignment procedures shall continue).

The following additional conditional requirement shall apply to the STP:

**CR4-123** [132] As a per-Bcc option, the STP shall provide an option to stop or continue alignment procedures after T1.111.4/T19 expires. This option shall be provisionable on a per-node basis.

**R4-124** [133] The STP shall perform link set activation as discussed in Section 12.2.4 in T1.111.4 of GR-246-CORE.

The filtering procedure for links oscillating in and out of service is included in GR-246-CORE. The differences between GR-246-CORE and this document are as follows: although GR-246-CORE discusses two filtering algorithms, one of the methods is preferred for a Bcc network as indicated below; unlike GR-246-CORE, requirements in Section 6 state the default values for timers associated with the filtering algorithms.

**R4-125** [134] An STP shall provide one of the two link oscillation filter algorithms described in Section 12.2.2 of T1.111.4 of GR-246-CORE. *Procedure A is preferred.*

**R4-126** [135] The alignment should be delayed under the scenarios described in Section 12.2.2 in T1.111.4 of GR-246-CORE, with the following exceptions:

- If the link was manually removed from service
- If the link is put back in service manually
- If the link is connected to an adjacent node that is going through the node restart procedures
- The STP fails (and then uses the node restart procedures).

Note, the alignment should be delayed as described above, even if

- At least one destination is isolated as a result of the link being out of service
- If one or more of the other links in the (combined) link set are congested when the link is out-of-service.
When maintenance is notified of a link failure, if the restoral of the link will be delayed, the STP shall include an indication that restoral will be delayed and the amount of the delay (i.e., the remainder of T1.111.4/T32 or T1.111.4/T34) in the report.

4.2.4.11 Introduction to Cluster Management

This subsection serves as an introduction to cluster management requirements in subsequent subsections on signaling route management procedures: transfer-prohibited, transfer-restricted, transfer-allowed and signaling-route-set test. In particular, it discusses an internal logical data model for an STP in terms of which many requirements throughout the document are stated. A detailed review of cluster management is provided in Appendix D.

Two models of cluster routing and management are discussed in this section. The model of cluster routing and management considered in issues prior to and including TR-NWT-000082, Issue 4 of this document limited the use of cluster routing to situations when every member of the cluster was accessible via the same route set. Thus, if an E-link was deployed to a single member of a remote cluster, cluster routing could not be performed. This model is known as the *cluster routing and management* (CRM) model. Requirements discussed in Section 4.2.3.2.2 and the following subsections support the interworking of E-links and cluster routing and management. According to these requirements, member route sets may be provisioned for members of a cluster for which a cluster route set is also provisioned. For this enhanced model of cluster routing and management, requirements for transfer-prohibited, transfer-restricted, transfer-allowed procedures have been extended to allow both cluster and member routes to be present for the same cluster. This enhanced model is hereafter referred as the *cluster routing and management diversity* (CRMD), or simply as the *diversity model*. The requirements associated with the diversity model but not with the cluster routing and management model are given separately from the requirements associated with both models. In other words, all the requirements which are not explicitly indicated as the diversity model requirements are applicable to both models. The requirements associated with the diversity model are conditional on a per-Bcc basis and are indicated by *(R) CRMD*. Some of the specifications associated with the diversity model are left in the main text and they are always preceded by an explanation indicating their association with the model.

As a per-Bcc option, the STP shall provide the capability of performing full point code routing, as well as cluster routing (i.e., the STP must be capable of using cluster routing to reach one cluster, and still be capable of using full point code routing to members of another cluster), administerable on a per-cluster basis.

If the above conditional requirement is selected, it implies that, for a given cluster, *either* full point code routing or cluster routing will be provisioned, but not both. The next
conditional requirement, if selected, allows an STP to provision both cluster routes and members routes in the same cluster.

**CR4-129** [138] As a per-Bcc option, the STP shall provide the capability of performing cluster routing and management diversity, in which both member route sets and a cluster route set are administered in the same cluster. The STP shall be capable of performing member (full point code) routing or cluster routing or a combination of member and cluster routing toward a cluster of signaling points.

### 4.2.4.11.1 Terminology

This section considers the terminology used in discussing cluster management.

The term *destination* is used to refer both to an individual SP (or a mated pair of STPs addressed via a Capability Code) and a cluster of SPs.

In referring to the affected destination in TFx messages, the term *affected SP* will be used to denote two possible cases: when the affected destination is an individual SP, and when the affected destination is a mated pair of STPs addressed via a Capability Code. (An STP sending or receiving a TFx message will not know whether the affected destination is a PC or Capability Code).

A member route set and a cluster route set are *associated* if the Network ID and Network Cluster fields of the Point Codes of the destinations are identical.

**R4-130** [139] The STP shall maintain two statuses for each route to a destination. First, it shall maintain information regarding whether the link set corresponding to the route is *available* or *unavailable*. Second, it shall maintain information regarding the routing status for each node or cluster accessible via the route, as indicated by the last received signaling transfer message (TFx or TCx message) for that route. These two statuses shall be independent from one another and shall be used in determining whether traffic to a particular destination can use the concerned route.

These two statuses are described below:

**Signaling Link Status:**

A link is said to be *available* if it can be used to carry signaling traffic. Otherwise, it is said to be *unavailable*.

A link is said to be *local* to a node if it is connected to the node.

**Signaling Route Status:**
The status of a signaling route (here, a single link set is implied) to a destination is dependent not only on the condition of the local links in that route, but also on the status indicated in TFx or TCx message that was last received for the route concerning the destination.

The following definitions are used in the subsequent sections to explain the last signaling route management message received on a route.

A cluster is said to be marked
- \textit{allowed} on a route if a TCA message corresponding to the cluster was last received for that route.
- \textit{restricted} on a route if a TCR message corresponding to the cluster was last received for that route.
- \textit{prohibited} on a route if a TCP message corresponding to the cluster was last received for that route.

A member is said to be marked
- \textit{allowed} on a route if a TFA corresponding to the member, or in some cases, a TCA message (see Section 4.2.4.13) corresponding to the cluster to which the member belongs, was last received for that route.
- \textit{restricted} on a route if a TFR corresponding to the member, or in some cases, a TCR message (see Section 4.2.4.14) corresponding to the cluster to which the member belongs, was last received for that route.
- \textit{prohibited} on a route if a TFP corresponding to the member, or in some cases, a TCP message (see Section 4.2.4.12) corresponding to the cluster to which the member belongs, was last received for that route.

A signaling route to a destination (cluster or member) is
- \textit{available} if the local link(s) in the route can be used to carry the concerned signaling traffic \textit{and} the destination is marked allowed on the route.
- \textit{unavailable} if the local link(s) in the route can not be used to carry the concerned signaling traffic \textit{or} the destination is marked prohibited on the route.
- \textit{restricted} if the local link(s) in the route can be used to carry signaling traffic \textit{and} the destination is marked restricted on the route.

\textbf{Overall Routing Status:}

The following definitions should be referenced in determining the status of a destination from a signaling point's perspective across all possible routes from the signaling point and are used as the basis for determining which signaling route management messages should be sent to adjacent nodes.

If the destination is a cluster, the following status definitions apply:
• A cluster is inaccessible if each route in the cluster route set is unavailable. For cluster routing and management diversity, the definition is extended to comprise the status of any associated member routes sets: A cluster is inaccessible if each route in all associated member route sets is unavailable, and each route in the cluster route set is unavailable.

• A cluster is accessible if the conditions for inaccessibility do not hold. Specifically, a cluster is
  — Accessible via normal route(s) if any normal route in the cluster route set is available or restricted. For cluster routing and management diversity, the definition is extended and thus a cluster is said to be accessible via normal route(s) if any normal route in any associated member route set is available or restricted, or if any normal route in the cluster route set is available or restricted. (For both the cluster routing and management and the diversity models, a cluster, from an STP’s perspective, is accessible via normal route[s] if the STP can use the normal route[s] to carry the concerned signaling traffic for at least one member of the cluster.)
  — Only accessible via alternate route(s) if all normal cluster routes are unavailable and any cluster route other than the normal cluster routes is available or restricted. For cluster routing and management diversity, the definition is extended and therefore a cluster is said to be accessible only via alternate route(s) if all normal routes in the cluster route set and all associated member route sets are unavailable and any route other than the normal route(s) in the cluster route set or any associated member route set is available or restricted.

If the destination is a member, the following status definitions apply:

• A member is inaccessible if one of the following three situations exists:
  1. each route in the member route set is unavailable
  2. the member is marked prohibited on the x-list for each available or restricted route in the cluster route set and, in case of cluster routing and management diversity, no associated member route set is provisioned for the member
  3. if all routes in the cluster route set are unavailable, and, in case of cluster routing and management diversity, an associated member route set is not provisioned for the member.

• A member is accessible if the conditions for inaccessibility do not hold. The following definitions are true for both the cluster routing and management and the diversity models. A member is
  — accessible via normal route(s) if any normal route in the member route set is available or restricted, or, if no member route set is provisioned, any normal route in the cluster route set is available or restricted, and the member is not marked prohibited on the x-list for that cluster for that route. (That is, a member is
accessible via normal route[s] as long as normal route[s] can be used to carry the concerned signaling traffic.)

— only accessible via alternate route(s) if it is accessible, but not via normal route(s).

Existential Member:

The treatment of a particular cluster as one network entity by cluster management procedures rather than as a group of signaling points may result in the treatment of all existent and non-existent members of the cluster equally. To clarify the distinction between these two types of members, the term existent member is used in subsequent sections and in Appendix D to indicate a member of the cluster which physically exists in the network. Similarly, the term non-existent (ghost) member is used to refer to non-existent members which may be processed by cluster management procedures due to treatment of a cluster as a single entity.

4.2.4.11.2 Route Management

When cluster routing (see Section 4.2.3.2) is used in the network, CCS nodes, in particular STPs, must be able to perform cluster management functions. For STPs, these functions can be grouped as follows:

1. Processing of TCP, TCA, TCR, and signaling-route-set-cluster-test messages received from adjacent nodes (note that an STP must be able to process TCx messages even if there is not a single cluster routing entry in its MTP routing table)

2. Generating TCP, TCA, TCR messages for a cluster of SPs towards which cluster routing is performed and possibly in other cases (implementation of other cases is left as a supplier option)


4. When cluster routing is performed towards a particular cluster, maintaining route statuses of cluster members (for which member routing is not performed) when such statuses are more restrictive than the status of the affected route to the cluster, e.g., status of a route to a member may be unavailable while the cluster route status is available or restricted (this is done by means of an x-list discussed below)

5. Processing of TFx and signaling-route-set-test messages when cluster routing is performed towards the affected or tested destination

6. Updating adjacent nodes on cluster member statuses after sending TCA or TCR messages (by sending TFP and TFR messages regarding prohibited and restricted members after a TCA message and by sending TFP messages regarding prohibited members after a TCR message [under certain circumstances, sending TFP and TFR messages depend on the supplier option of maintaining x-lists, as described later in Section 4.2.4.12.3]).
Of the six groups listed above, GR-246-CORE considers functions in groups 1, 2, and 3, but, for group 2, it considers the generation of TCx messages only when the same route set is used for all members of the cluster. Thus, the subsequent signaling route management sections discuss the other cases when TCx messages may be sent as a supplier option and functions in groups 4, 5, and 6.

Although functions in groups 1, 2, and 3 are considered a network option in GR-246-CORE, they are required in Bcc networks as stated in Requirement R4-131 [140].

**R4-131** [140] An STP shall be able to perform cluster management functions listed under groups 1, 2, and 3 above that are described in GR-246-CORE.

In discussing the functions in groups 4 through 6, it is convenient to assume that an STP uses a particular internal logical data model for maintaining routing statuses. The “x-list” model used in this document assumes that when an STP has a cluster route set provisioned for a particular cluster, it also maintains the route status for individual cluster members on a per-route basis in a dynamic routing exception list, denoted as an x-list. When a combined link set represents two routes of equal priority to a cluster, an x-list is maintained for each route. Each x-list is thus associated with a particular cluster and route. Information regarding a member is only maintained on an x-list if a member route set is not provisioned for the affected member (i.e., an x-list keeps records of statuses of that route to members for which member routing is not performed). Throughout this document, requirements associated with cluster routing and management are often stated in terms of the x-lists. However, **such requirements are intended to be, and should be interpreted as, applicable only to the externally visible behavior of the STP.** References to the x-lists are not intended to construe a particular internal STP implementation of cluster routing and management or internal STP data storage.

Although the primary objective of an x-list is to maintain statuses of members on a cluster route that are more restrictive than the status of the cluster route, in some situations it is permissible and possibly advantageous to keep statuses of individual members on the x-list even if these statuses are equally restrictive as the cluster route status. Specific procedures for the maintenance of the x-list are discussed in subsequent signaling route management sections and a detailed review is presented in Appendix D.

It is possible that an x-list entry will appear for a PC that does not exist. Such an entry may stay on the x-list until the entry for the PC on the x-list is manually removed (see Section 4.2.4.15.2). An entry may also be removed from the x-list automatically as discussed in Requirement R4-132 [141].

**R4-132** [141] The STP shall contain a timer (T_x-list) that is started when a PC is placed on a cluster's x-list, and runs until the status of the route to the PC changes. If the timer expires before the status changes, and if no traffic addressed for the PC was routed through the STP while the timer was running, then the PC entry shall be removed from the x-list (thus inheriting the status of the cluster), the signaling-route-set-test procedures for the PC
shall be terminated, and the STP shall notify management of the suspected error condition. (Note that it is not necessary to perform controlled rerouting since there is no traffic for the affected PC.) If the timer expires before the status changes, and if traffic addressed for the PC did arrive at the STP while the timer was running, then the timer shall be restarted. The value of the timer shall be provisionable on an office basis. A range between 20 minutes and 24 hours is suggested, with a default of 1 hour.

Requirement **R4-132** [141] and Conditional Requirement **CR4-134** [143] apply to the provisioning of options related to cluster network management.

**R4-133** [142] A Bcc shall be able to administer, on a per-cluster basis (i.e., this data should be recent changeable), whether or not an x-list is kept for any cluster for which the STP has a cluster route set provisioned.

By specifying the clusters for which an x-list is kept, the Bcc will be able to reduce the STP resources necessary for maintaining the x-lists.

**CR4-134** [143] As a per-Bcc option, a Bcc shall be able to administer on a per-cluster basis whether or not transfer-prohibited (TFP), transfer-allowed (TFA), transfer-cluster-prohibited (TCP), and transfer-cluster-allowed (TCA) messages will be broadcast about clusters and cluster members to which the STP performs cluster routing or, in case of cluster routing and management diversity, a combination of cluster routing and member routing. (It should be noted that broadcast of TCR and TFR messages regarding a cluster or members of a cluster is not Bcc-optional and therefore their broadcast is not affected by this conditional requirement.) For a cluster for which the messages will not be broadcast, the STP shall still perform the following network management functions with respect to that cluster and any cluster members on the x-lists: send response mode TFP/TCP messages, send TFC messages, respond to signaling-route-set-test/signaling-route-set-congestion-test messages, and originate signaling-route-set-test/signaling-route-set-congestion-test messages.

By specifying the clusters for which the network management messages are broadcast, the Bcc will be able to reduce the STP resources necessary for broadcasting such messages.

Requirements **R4-135** [144] and **R4-136** [145] address the use of member and cluster route sets when both are provisioned in the same cluster:

**R4-135** [144] **CRMD** The STP shall consult a member route set, if it exists, to determine an outgoing route over which to send a message.

**R4-136** [145] **CRMD** If no member route set exists, an STP shall consult the cluster route set, to determine an outgoing route over which to send a message.
4.2.4.12 Transfer-Prohibited Procedure

This section considers both TFP and TCP messages. An STP sends a TFP/TCP message to notify an adjacent signaling node that it is unable to route messages to the specified destination (referred to as the affected destination). When the affected destination is an individual SP, a TFP message is sent, and a TCP message is sent if the destination is a cluster of SPs. A TFP/TCP is also sent to notify adjacent nodes that messages for the affected destination should not be sent to the STP because the route might be circular. In the latter case, the TFP/TCP is referred to as a preventive TFP/TCP.

R4-137 [146] An STP shall initiate and perform the transfer-prohibited procedure as discussed in Section 13.2 in T1.111.4 of GR-246-CORE.

In addition, the STP shall also conform to the requirements discussed below.

Several aspects of the description of the transfer-prohibited procedure in GR-246-CORE are clarified below:

- One of the actions that may be taken by an STP upon receiving a TFP/TCP message is not stated explicitly in Section 13.2 in T1.111.4 of GR-246-CORE although it is indicated in an Specification and Description Language (SDL) (the ITU-T [formerly CCITT] Specification and Description Language) diagram (see Section 16 in T1.111.4 of GR-246-CORE). Requirement R4-138 [147] describes this action.

R4-138 [147] When an STP receives a TFP or TCP message and the STP performs full PC routing or cluster routing, respectively, towards the affected destination, the STP shall mark the destination as prohibited on the affected route unless it was already marked so. If the affected destination is a cluster and the STP only performs full PC routing towards members of that cluster, the STP shall mark the members of that cluster (that appear in the MTP routing table) prohibited on the affected route, unless they were already marked so. This action shall be taken independently of whether the affected route is the current route or not.

Note that if the affected destination is an individual SP and the STP only performs cluster routing towards that destination, the STP shall take the actions as discussed in Section 4.2.4.12.3. As indicated in that section, an STP may change the status of the route to the affected destination in the x-list associated with the affected cluster and route. These actions are not discussed in GR-246-CORE.

- One of the cases when TFP/TCP messages are sent by an STP is in response to a signaling-route-set-test message. This case is not mentioned in Section 13.2 in T1.111.4 of GR-246-CORE, but it is mentioned in Section 13.5 which discusses the signaling-route-set-test procedure.

- GR-246-CORE does not state whether a TFP or TCP message should be sent when an STP receives a message addressed to a destination for which no MTP routing data is
provisioned. Requirements R4-139 [148] through R4-143 [152] describe the actions an STP should perform in such a situation:

**R4-139** [148] If a message is received addressed to a particular destination \( a \), and the following two conditions apply:

... 1. The STP does not have a member route set provisioned for destination \( a \), nor a cluster route set for the cluster of which destination \( a \) is a member, but

... 2. The STP does have a member route set provisioned (including if the network and cluster identifiers equal that of any of the STP's PCs) for a different member of the same cluster as \( a \),

... then the STP shall send a TFP message about destination \( a \) to the node from which the message was received.

**R4-140** [149] If a message is received addressed to a particular destination \( a \), and the following two conditions apply:

... 1. The STP does not have a member route set provisioned for destination \( a \), nor a cluster route set for the cluster of which destination \( a \) is a member, and

... 2. The STP does not have a member route set provisioned (the network and cluster identifiers are not equal to any of the network and cluster identifiers of the STP's PCs) for any other members of the same cluster as \( a \),

... then the STP shall send a TCP message about destination \( a \) to the node from which the message was received. As a non-preferred option, the STP may send a TFP message instead of a TCP.

- **GR-246-CORE** assumes one PC per CCS node and does not consider the possibility of an SPCS which is assigned multiple PCs (see Section 4.2.3.1). Requirements R4-141 [150], R4-142 [151], and R4-143 [152] apply:

**R4-141** [150] An STP may receive a TFP message about a primary or secondary PC assigned to an adjacent SPCS with multiple PCs. The STP should treat each PC as if it were an independent signaling point and hence shall only update the route status of the affected PC.

**R4-142** [151] When an adjacent multiple PC SPCS becomes inaccessible, the STP shall broadcast a TFP message about both primary and secondary PCs. (It is assumed that when a multiple PC SPCS becomes inaccessible, both primary and secondary PCs are inaccessible, i.e., it is not possible for only some PCs to be accessible while others are not.)
R4-143 When sending a TFP/TCP to a multiple PC SPCS, the STP shall use the primary PC as the DPC of the message.

Additional requirements for the transfer-prohibited procedure are considered in the subsections below. They consist of requirements that do not appear in GR-246-CORE and those that are not addressed in GR-246-CORE in detail. The additional requirements can be categorized as follows:

- Broadcasting TFP/TCP Message
- Preventive TFP/TCP
- Sending Response Mode TFP/TCP
- Actions Taken Upon Receipt of TFP/TCP
- Cluster Management
- Performance Requirements.

4.2.4.12.1 Broadcasting TFP/TCP Message

A TFP/TCP message may be broadcast when an STP recognizes that a destination has become inaccessible. This may happen upon receipt of a TFP/TCP message for the last available route to that destination or because of link set outage. GR-246-CORE states that a TFP/TCP message shall be broadcast if the inaccessible destination “has been designated (by the administration of the network to which the STP belongs) as one for which the STP should broadcast TFP/TCP message,” i.e., it leaves the choice of when a TFP/TCP should be broadcast to the network administrator. The rules that shall apply to Bccs are stated below:

R4-144 Unless an option to deactivate broadcast method (see the conditional requirement in Section 4.2.4.11.2) is selected for an inaccessible cluster, an STP shall broadcast a TCP message to all accessible adjacent SPs whenever it first recognizes that the cluster has become inaccessible.

R4-145 CRMD In accordance with the definition of an inaccessible cluster in Section 4.2.4.11.1, an STP shall not broadcast a TCP message for a cluster if an associated member route set is provisioned, and the status of the member, as indicated in that route set, is accessible. (This is not an exception to the broadcast TCP requirement; it is a reflection of the definition of an inaccessible cluster.)

R4-146 Unless a TCP message is broadcast in accordance with a previous requirement, an STP shall broadcast a TFP message about an inaccessible...
member when it first recognizes that the member has become inaccessible and the following conditions are true:

… 1. The STP believes that the concerned member is an existent member because a member route set is provisioned for the member, or it becomes inaccessible as a result of being placed on or remaining on an x-list.

… 2. The option to deactivate broadcast mode is not selected for the cluster of which the inaccessible destination is a member (see the conditional requirement in Section 4.2.4.11.2).

R4-147  [156] For any single failure condition causing the inaccessibility of one or more destinations (i.e., link set failures or receipt of TFP/TCP messages), an STP that broadcasts TFP/TCP messages as specified in requirement R4-146 [155] may cease broadcasting, regarding all destinations made inaccessible by the single failure condition, after the expiry of a timer $T_{brdcst}$. Timer $T_{brdcst}$ is started upon detection of the failure condition. ($T_{brdcst}$ has a user setable range of 0 to 15 seconds and a default of 7.0 seconds.)

If a TFP/TCP message is not broadcast in an exceptional case listed above, the STP shall be able to send TFP/TCP messages by the response method immediately after the destination becomes inaccessible, i.e., it shall not wait for the timer $T_{1.111.4}/T8$.

According to GR-246-CORE, a TFP/TCP message should be broadcast across a network boundary according to a bilateral agreement between the network administrators. If the agreement is not to broadcast, TFP/TCP messages for any affected destination shall be sent by the response method only except when the affected destination is the mated STP. If the affected destination is the mated STP, the TFP message must be broadcast across the network boundary to ensure that, in a case when the mated STP becomes isolated from the gateway STP(s) in the foreign network, the foreign gateway STP(s) perform the MTP restart procedure with respect to the mated STP after the latter recovers. If the TFP message were not broadcast, it would be possible for the isolation to occur without the foreign gateway STPs being aware of it. Note that the exceptional case when the TFP broadcast across a network boundary is required, i.e., when the affected destination is the mated STP, is not mentioned in GR-246-CORE.

According to the following conditional requirements, as a Bcc option, a gateway STP should have a capability not to broadcast TFP/TCP messages across a network boundary except when the affected destination is the mated STP. In addition, a gateway STP should have a provisionable on/off switch for such broadcasts.

CR4-148  [157] As a per-Bcc option, a gateway STP shall not broadcast a TFP/TCP message for all affected destinations across a network boundary except when the affected destination is the mated STP. (Note that the STP shall
still broadcast a TFP/TCP message in the Bcc network.) If the affected
destination is the mated STP, a TFP/TCP shall be broadcast across a
network boundary. A link set is considered to be crossing a network
boundary if the Network Identifier of the far end STP differs from the STP
broadcasting the TFP/TCP message. If the TFP/TCP is not broadcast
across a network boundary, the STP shall be able to send TFP/TCP
messages across the network boundary by the response method
immediately after the broadcast within the Bcc network, i.e., it shall not
wait for the time T1.111.4/T8.

CR4-149 [158] As a per-Bcc option, a gateway STP shall provide a capability to
turn on or off the broadcast of TFP/TCP messages across a network
boundary. The on/off switch for broadcasting TFP/TCP messages across a
network boundary shall be provisionable on a per-link-set basis. (The on/
off switch must be provisionable for every link set, not just a link set
leading to another network.) If the switch is provisioned “off” for a
particular link set, a TFP/TCP message for all affected destinations shall
not be sent to the STP at the far end of that link set during a broadcast
except when the affected destination is the mated STP (it shall be sent for
the mated STP); conversely, if the switch is provisioned “on,” the gateway
STP shall send the TFP/TCP message. For any link set, the default value
shall be set to “off” if the link set crosses a network boundary, and to “on”
otherwise. A link set is considered to be crossing a network boundary
according to the rule stated in the conditional requirement above.

4.2.4.12.2 Preventive TFP/TCP

The term preventive TFP/TCP refers to a TFP/TCP sent to prevent circular routing. An STP
sends a preventive TFP/TCP to an adjacent STP to inform the latter that traffic to the
affected destination should not be routed through the sender of the TFP/TCP message
because such routing may be circular. The current issue of GR-246-CORE states several
cases when a preventive TFP/TCP is sent, the first of which is:

• A TFP/TCP is sent by STP Y to adjacent STP Z when STP Y starts to route traffic,
e.g., at changeover, changeback, forced or controlled rerouting, to the affected
destination via adjacent STP Z not currently used for such traffic.

The remaining cases when a preventive TFP/TCP is sent are not discussed in detail in GR-
246-CORE and hence are considered below.

Preventive TFP/TCPs must be sent under the following circumstances to eliminate the
possibility of a circular loop:

• When an STP begins using a lower priority route through another STP to a particular
destination. The STP must send preventive TFP/TCPs to any accessible adjacent STPs
that provide an alternate route of higher priority to force those adjacent STPs to use their lower priority route as well, and NOT send traffic to the STP sending the preventive TFP/TCP for the affected destination.

- It may also be necessary to send preventive TFP/TCPs to other adjacent STPs when complex routing schemes are used (e.g., when three STP pairs are interconnected and a CCSSO has A-links and two sets of E-links deployed to those STPs). In this case, when an STP begins using a lower priority route through an STP (pair) for a particular destination, a preventive TFP/TCP may need to be sent to some adjacent STPs that route through that STP for the affected destination. Note, this second case is not supported by the requirements since Bcc networks do not plan to utilize the architectures or routing schemes which make this capability necessary.

For more information on the motivation for these requirements see Appendix A. A requirement for the first additional case when preventive TFP/TCP messages are sent is stated below.

R4-150 [159] When an STP begins to divert traffic for a particular destination to a lower priority route through an adjacent STP, the STP shall send a preventive TFP/TCP message for that destination to all accessible adjacent STPs on alternate routes of higher priority to the affected destination. As a supplier option, the STP may start a timer T1.111.4/T8 corresponding to the affected destination.

During an MTP restart procedure, an STP may start sending traffic to a particular destination on a route other than the normal one. If so, it must also send preventive TFP/TCPs mentioned in the requirement above as if it was diverting traffic from the normal route to the route being used. This is indicated in Section 9.1 and 13.2.2 (1) in T1.111.4 of GR-246-CORE.

For a variety of reasons, e.g., message loss or STP overload, a preventive TFP/TCP may not be acted upon by an adjacent STP. That adjacent STP may then continue to send traffic for the affected destination over the route for which a preventive TFP/TCP applies. GR-246-CORE does not explicitly state the disposition of messages for the affected destination that are received from such adjacent STP. The appropriate action in a Bcc network is discussed below.

To help ensure that circular routing does not occur even if a preventive TFP/TCP is not acted upon, an STP must discard messages addressed to the affected destination and received from adjacent STPs which is on the currently used route to the destination of the message and/or to which the preventive TFP/TCP was sent. Specifically, the STP must check each message arriving on a link set at the far-end of which is on the currently used route to the destination of the message and/or which is an STP to which a preventive TFP/TCP was sent; if a received message is addressed to the affected destination, it should be discarded. Since reception of such a message indicates that a preventive TFP/TCP may not
have been received and acted upon, the STP may resend the preventive TFP/TCP by the response method (see the following).

STP actions in checking for messages indicating the presence of circular routing are stated in Requirement R4-151 [160]. (As mentioned in Section 4.2.3.4, such STP actions constitute a new message distribution and discrimination function for the STP.)

R4-151 [160] When an STP receives a message for a destination from an adjacent STP which is on the currently used route to the destination of the message and/or to which a preventive TFP/TCP regarding that destination or cluster, of which the destination is a member, was sent, the STP shall discard the received message. The STP shall also resend the preventive TFP/TCP to that adjacent STP if the timer T1.111.4/T8, corresponding to the TFP/TCP previously sent, is not running. As a supplier option, the timer T1.111.4/T8 may be restarted when a TFP/TCP message is resent. The restarted timer shall apply only to the STP to which the TFP/TCP message was resent, i.e., it shall inhibit sending of additional TFP/TCP messages to that STP only.

Note that the current issue of GR-246-CORE does not state that the timer T1.111.4/T8 may be started when a preventive TFP/TCP is sent. In a Bcc network, the timer T1.111.4/T8 may be started, as a supplier option, for the preventive TFP/TCP messages. Also, the current issue of GR-246-CORE does not state that preventive TFPs should be sent in the response mode for messages received from an adjacent signaling transfer point which is on the currently used route to the destination of the message.

4.2.4.12.3 Requirements Associated With Cluster Management

This subsection considers additional requirements for the transfer-prohibited procedure associated with cluster management. Note that a requirement related to cluster management also appears in Section 4.2.4.12.1. For an overall description of cluster management, see Appendix D.

The following two requirements address the use of response mode TFP/TCP messages, when cluster routing and management are being performed for the affected destination.

R4-152 [161] If the STP receives a message from an adjacent node destined for a cluster that is inaccessible in accordance with the definition stated in Section 4.2.4.11.1, then it shall send a TCP message about the inaccessible cluster to the adjacent node if a corresponding timer T1.111.4/T8 is not running.

R4-153 [162] If the STP receives a message from an adjacent node destined for a member that is inaccessible in accordance with the definition stated in
Section 4.2.4.11.1, then it shall send a TFP message about the inaccessible member to the adjacent node if a corresponding timer T1.111.4/T8 is not running, and if a TCP message is not sent according to the previous requirement.

An STP may send a TCP message not only under the conditions described previously and in Section 13.2 in T1.111.4 of GR-246-CORE, but also in cases when it performs full PC routing rather than cluster routing for a local or remote cluster. Specifically, if an STP only performs full PC routing to a cluster and it recognizes that it can not route messages to any member of that cluster, it may send a TCP message for the cluster. This would reduce the quantity of resulting signaling-route-set-test messages from the nodes to which it sends the TCP message. The functionality of sending the TCP message under these circumstances is optional for the STP, i.e., the choice is left to the STP supplier. See also related paragraphs for TCR and TCA messages in Sections 4.2.4.14.2 and 4.2.4.13.2, respectively.

Requirement **R4-154 [163]** addresses the need for an STP to inform adjacent nodes about the cluster members with a status more restrictive than the status of the cluster after a TCA or TCR message is sent (broadcast or response method). The motivation for this requirement is described in Appendix D, Section D.5.3. The requirement considers inaccessible members of the affected cluster only, but there is a similar requirement in Section 4.2.4.14.2 for members accessible via alternate route(s).

**R4-154 [163]** If an STP sends (broadcast or response method) a TCA or TCR message concerning a remote cluster to an adjacent node and some members of that cluster are inaccessible, the STP shall be able to inform the adjacent node of the inaccessible members of the cluster, in one of the following two ways:

... • It shall send a TFP message for each inaccessible member, immediately after each TCA or TCR message

... • It shall cancel all running T1.111.4/T8 timers for the inaccessible members of the cluster, if there are any, and be able to send response mode TFP messages immediately after the broadcast of a TCA or TCR message.

When an STP receives a TCP message, it marks the cluster as prohibited on the affected cluster route if the status of the cluster was previously marked as restricted or allowed. In the case of cluster routing and management diversity, if, in addition, an associated member route set is provisioned and the affected route is in the member route set, then the STP marks the member as prohibited on the route. If the cluster was already marked prohibited, no action is taken. These actions are similar to those taken upon receipt of a TFP message for an individual SP towards which full PC routing is performed.

If an STP marks the cluster as prohibited on a route upon receipt of a TCP message, the STP may either clear the x-list associated with the affected cluster and route (i.e., it may remove all entries from the x-list) or it may leave members marked prohibited on the x-list, and
change restricted members to prohibited (i.e., keep the x-list entries while the cluster is marked prohibited over that route). (Note that the STP should not receive any TFP, TFA, or TFR messages updating the status of cluster members for the affected route while the cluster is marked prohibited over that route.) The argument for keeping cluster members on the x-list is that the status of these members will not change if the status of the cluster route changes after a short time; the argument against is that the member statuses will change if the status of the cluster route remains the same for a long time. The choice of whether to keep or remove cluster members from the x-list is left to the STP supplier. In either case, the STP shall stop sending signaling-route-set-test messages for members of the cluster and shall start sending a cluster-signaling-route-set-prohibited-test message periodically while the cluster is marked prohibited on the route.

Requirement R4-155 [164] considers STP actions upon receiving a TFP message for an individual SP towards which cluster routing is performed.

R4-155 [164] When a TFP is received at an STP and the STP is performing cluster routing for the prohibited destination, the STP shall perform the following actions independent of whether the affected route is the current route or not.

…

• If the cluster is marked restricted or allowed on the affected route, the STP shall add the prohibited PC to the x-list on that route if the PC was not already listed. If the affected PC was already listed as restricted, the restricted status shall be updated to prohibited. If the affected PC was already listed as prohibited, no action shall be taken.

…

• If the cluster is marked prohibited on the affected route, no action shall be taken.

Conditional Requirements R4-156 [165] and R4-157 [166] explain actions that an STP should take when it is equipped with cluster routing and management diversity capability for a cluster. These requirements apply if both member route sets and a cluster route set are provisioned in a cluster.

R4-156 [165] CRMD When a TCP is received at an STP, and the STP recognizes that a member route set is provisioned in the cluster (i.e., an associated member route set is provisioned), then, if the affected route is in the member route set, the STP shall mark the member as prohibited on the route, and start signaling-route-set-test procedure for the cluster.

R4-157 [166] CRMD When a TFP is received at an STP, and the STP recognizes that a member route set is provisioned in the cluster, as well as a cluster route set, then, if the affected route is in the member route set, the STP shall mark the member as prohibited on the member route, and start signaling-route-set-test procedures. No x-list entry is made in the cluster route.
Conditional Requirement CR4-158 [167] applies to the failure scenario when a member route in a member route set is available or restricted, but the routes in the cluster route set are unavailable. (For example, it applies to the scenario when an STP has available E-links for one member, but the B-links toward the cluster and the C-links toward its mate are unavailable.)

**CR4-158 [167]** If a message addressed to a particular destination \( a \) is received and the following four conditions apply:

1. The STP does not have a member route set provisioned for \( a \)
2. The STP has a member route set provisioned for a different member of the same cluster as \( a \), and the member with a member route set provisioned is accessible
3. The STP has a cluster route set provisioned for the cluster of which \( a \) is a member
4. Member \( a \) is inaccessible,

then the STP should send a response mode TFP message about inaccessible member \( a \), if a corresponding timer T1.111.4/T8 is not running.

### 4.2.4.12.4 Performance Requirements

The following performance requirements shall apply to an STP for the transfer-prohibited procedure, which includes the preventive TFP procedure:

**R4-159 [168]** An STP shall be able to *start broadcasting* (placing a TFP/TCP message in the transmit buffer) to an accessible adjacent SP within 0.25 seconds of the trigger event that caused the broadcast.

A trigger event may be:

- Link set outage that results in a destination becoming inaccessible
- TFP/TCP message is received resulting in a destination becoming inaccessible
- Circular routing situations as described in Section 4.2.4.12.2.

**R4-160 [169]** The subsequent broadcast of the TFP/TCP message, including the preventive TFP/TCP message, to each additional node shall not be more than an average of 10 milliseconds apart.
R4-161 [170] An STP shall send a TFP/TCP message by the response method within 0.1 seconds of the trigger event that caused the message to be sent unless the timer T1.111.4/T8 is running.

A trigger event may be:

- Receipt of a message for an inaccessible destination
- Receipt of a message addressed to destination X from an STP to which a preventive TFP/TCP for destination X has been sent (a preventive TFP/TCP is resent in this case).

Related STP performance requirements are stated in the sections on forced rerouting. They specify the time within which forced rerouting procedure shall be performed by an STP after a receipt of a TFP/TCP message. A related STP performance requirement is also stated in Section 4.2.4.15.6 on the signaling-route-set-test procedure. It specifies the time within which a TFP/TCP message must be sent in response to a signaling-route-set-test message.

4.2.4.13 Transfer-Allowed Procedure

This section considers both TFA and TCA messages. A TFA/TCA message is sent by an STP to notify adjacent nodes that the normal signaling route to a destination specified in the message (referred to as the affected destination) is available or restricted. When the affected destination is an individual SP, a TFA message is sent, and a TCA is sent for a cluster of SPs.

R4-162 [171] An STP shall initiate and perform the transfer-allowed procedure as discussed in Section 13.3 in T1.111.4 of GR-246-CORE. In addition, the STP shall also conform to the requirements discussed below.

Several aspects of the description of the transfer-allowed procedure in GR-246-CORE are clarified below:

- One of the actions that may be taken by an STP upon receiving a TFA/TCA message is not stated explicitly in Section 13.3 in T1.111.4 of GR-246-CORE although it is indicated in an SDL (the ITU-T [formerly CCITT] Specification and Description Language) diagram (see section 16 in T1.111.4 of TR-NWT-246). Requirement R4-163 [172] describes this action.

R4-163 [172] When an STP receives a TFA or TCA message and the STP performs full PC routing or cluster routing respectively towards the affected destination, the STP shall mark the status of the affected destination as allowed on the affected route unless it was already marked so, whether that route is the current route or not.

If the affected destination is a cluster (i.e., if a TCA message is received) and the STP only performs full PC routing towards members of that cluster, the STP shall mark the
status of all members of that cluster (that appear in the MTP routing table) as allowed on the affected route unless they were already marked so, independently of whether the affected route is the current route or not.

Note that if the affected destination is an individual SP and the STP performs cluster routing towards that destination, the STP shall take the actions as discussed in Section 4.2.4.13.2. As indicated in that section, an STP may change the status of the affected destination in the x-list associated with the affected cluster and route. These actions are not discussed in GR-246-CORE.

- One of the cases when TFA/TCA messages are sent by an STP is in response to a signaling-route-set-test message. This case is not mentioned in Section 13.3 in T1.111.4 of GR-246-CORE, although it is mentioned in Section 13.5 which discusses the signaling-route-set-test procedure.

- GR-246-CORE assumes one PC per CCS node and does not consider the possibility of an SPCS which is assigned multiple PCs (see Section 4.2.3.1). Requirements R4-164 [173] through R4-167 [176] apply:

R4-164 [173] An STP may receive a TFA message about a primary or secondary PC assigned to an adjacent SPCS with multiple PCs. The STP should treat each PC as if it were an independent signaling point and hence shall only update the route status of the affected PC.

R4-165 [174] When an adjacent multiple PC SPCS becomes accessible via the normal route, the STP should broadcast a TFA message about both primary and secondary PCs.

R4-166 [175] When sending a TFA/TCA to a multiple PC SPCS, the STP shall use the primary PC of the SPCS as the DPC of the message.

- As described in Section 4.2.4.12.2, preventive TFPs/TCPs may be sent by STP Y to adjacent STP Z to prevent circular routing. If STP Z subsequently sends a TFP or TFR to STP Y about the affected destination, a TFA should not be sent from STP Y to STP Z because this will cancel the effect of the original TFP (sent from STP Y to STP Z) and allow backrouting over the B-link if such a backroute were provisioned at STP Z.

R4-167 [176] An STP shall not send a TFA message to adjacent mated STPs Z or Z' when a combined B-link set from STP Y to STPs Z and Z' is used as the first priority route from STP Y to destination X and STP Y subsequently receives a TFP (or TFR) from STP Z or Z' about destination X (e.g., the A- and C- links to destination X have failed).

Additional requirements for the transfer-allowed procedure are considered in the following subsections. They consist of requirements that do not appear in GR-246-CORE and those
that GR-246-CORE does not address in detail. The additional requirements can be categorized as follows:

- Broadcasting TFA/TCA Message
- Cluster Management
- Performance Requirements.

4.2.4.13.1 Broadcasting TFA/TCA

A TFA/TCA message may be broadcast when an STP first recognizes that a destination becomes accessible via normal route(s). This may happen upon receipt of a TFA/TCA or TFR/TCR message for a normal route to that destination or because a link set corresponding to a normal route became available.

R4-168 [177] An STP shall broadcast a TFA message about a signaling point, in accordance with the definitions in Section 4.2.4.13.1, if the signaling point has become accessible via normal route(s) and the following conditions are true:

1. The STP believes that the concerned signaling point exists because a member route set is provisioned, or it becomes accessible via normal route(s) as a result of being removed from or remaining on an x-list.

2. The option to deactivate broadcast mode is not selected for the cluster of which the concerned signaling point is a member.

An STP also needs to inform its adjacent nodes about the members which are inaccessible or accessible only via the alternate route(s) (due to local link set failure(s)) after broadcasting a TCA message. The motivation for this is described in Appendix D, Section D.5.3, and the requirements associated with it is given in Sections 4.2.4.12.3 and 4.2.4.14.2.

The subsections below address two topics:

- The exceptional cases when a TFA/TCA message is not broadcast
- Pacing the broadcast of TFA/TCA messages.

A. Exceptional Cases When TFA/TCA Message Is Not Broadcast

Generally, an STP shall broadcast a TFA/TCA message to all accessible adjacent SPs (but not to the STP at the far end of the newly available or restricted normal route) whenever it recognizes that a destination first becomes available. The three exceptional cases are described below. An additional clarifying case related to cluster management is described in Section 4.2.4.13.2.
R4-169  [178] A TFA message is not broadcast if an option to deactivate broadcast mode (see conditional requirement in Section 4.2.4.11) is selected for the cluster of which the allowed SP is a member.

R4-170  [179] A TCA message is not broadcast if an option to deactivate broadcast mode (see conditional requirement in Section 4.2.4.11) is selected for the affected cluster.

To minimize the likelihood of congestion when the first link or first few links in a (combined) link set with 3 or more links become available, a TFA/TCA should not be broadcast for destinations which were not accessible via normal route(s) through the newly available normal (combined) link set if a sufficient number of links are not available in the (combined) link set. (A TFR/TCR may be broadcast instead of a TFA/TCA as discussed in Section 4.2.4.14.1 of this document.) Although this topic is discussed in the current issue of GR-246-CORE (see Sections 13.4.2 and 13.4.2A in T1.111.4), GR-246-CORE does not state specific criteria under which an STP refrains from a TFA/TCA broadcast or sending a TFA/TCA message in response to a signaling-route-set-test message. Such specific criteria for a Bcc network are considered below.

R4-171  [180] For A/E link sets with 3 or more links and B/D combined link sets with 3 or more links, when a previously unavailable normal (combined) link set becomes available, the STP shall consider the routes corresponding to that (combined) link set restricted (assuming no destination is marked prohibited on the routes corresponding to that link set), and refrain from sending TFA/TCA messages regarding the destinations accessible through the (combined) link set, while the number of available links in the (combined) link set is less than the minimum number of links considered to be adequate. The minimum number of links considered adequate shall be provisionable on a per-(combined)-link set basis (see requirement R4-172 [181]). When the number of available links becomes equal or exceeds the provisioned minimum number, the destinations using the route corresponding to the (combined) link set as their normal route shall be considered allowed (assuming no destination is marked prohibited on the routes corresponding to the link set). The STP shall inform the adjacent nodes of an allowed route status by responding to a signaling-route-set-test message (see Section 4.2.4.15). Note that in this case the STP shall not broadcast a TFA/TCA message.

Note that when the number of available links in the (combined) link set is equal to or exceeds the provisioned minimum number, the normal routes corresponding to this (combined) link set shall be considered available, even after the number of available links falls below the provisioned minimum. However, the danger of congestion criterion discussed in item (2) of Section 13.4.2 in T1.111.4 of GR-246-CORE may apply.
Requirement R4-172 [181] addresses the provisioning of the minimum number of links in a link set that will determine when the routes corresponding to the link set will be considered allowed.

**R4-172 [181]** For an A/E link set with 3 or more links and B/D combined link sets with 3 or more links, it shall be possible to provision the minimum number of links in the (combined) link set that need to be available for the route(s) corresponding to the (combined) link set to be considered available. The default value shall be set to half of the links in the (combined) link set for (combined) link sets with an even number of links or \([\text{number of links in (combined) link set} - 1]/2\) for odd number of links. (*Note, the corresponding data item is defined in Section 7.1.1.1.2.3 of GR-310-CORE on a link set basis and rules are given in Section 7.1.3.4 for handling the link set case.*)

### B. Pacing Broadcast of TFA/TCA Messages

In the past, when a destination which was previously accessible only via alternate routes(s) became accessible via normal route(s) and TFR/TCR messages had been broadcast regarding the destination, it was assumed that TFA/TCA messages about the destination could be broadcast at once. However, a nearly simultaneous broadcast of all TFA/TCA messages is likely to lead to congestion because the nodes receiving TFA/TCA messages will perform controlled rerouting nearly simultaneously. During the controlled rerouting traffic will be stored in buffers (for T1.111.4/T6) and then all of it may be released nearly at once for transmission over the newly available link set. To address this problem, the T1S1.3 standards working group has introduced an option to regulate the rate of TFA/TCA broadcasts. Although this is stated as an option in GR-246-CORE, the pacing of TFA/TCA messages during broadcast, and the specific method of pacing discussed below, are required in a Bcc network for A/E link sets and are a supplier option for combined B/D link sets.

**R4-173 [182]** When an A/E link set corresponding to a normal route becomes available, causing a destination that was accessible through alternate route(s) to become accessible through normal route(s) (it is assumed that a TFR/TCR had previously been sent), the STP shall pace the broadcast of TFA/TCA messages. The rate of broadcast shall be as follows:

- Up to 20% of the TFA/TCAs shall be sent when the destination becomes accessible via normal route(s). The TFA/TCA to the STP at the end of the current alternate route shall be sent first.

- The subsequent TFA/TCAs shall be sent in groups of up to 20% of the TFA/TCAs at the provisioned pacing rate.

**O4-174 [183]** It is desirable that Requirement R4-173 [182] for pacing the broadcast of TFA/TCA messages shall also apply when a combined B/D
link set corresponding to a normal route becomes available, causing a
destination that was accessible through alternate route(s) to become
accessible through normal route(s) (it is assumed that a TFR/TCR had
previously been sent).

**R4-175** [184] The pacing rate shall be provisionable in increments of 0.1 seconds,
with a range of 0 to 1 seconds, and a default of 1 second. If the value is set
to 0, no pacing shall be done (i.e., the TFA/TCA shall be broadcast without
any pacing). A single pacing rate shall be provisionable for both TFA/TCA
and TFR/TCR broadcasts. For the discussion of pacing of TFR/TCR
broadcasts, see Section 4.2.4.14.1C.

Note: If multiple destinations become accessible via normal route(s) at the same time, the
TFA/TCAs for each destination should be sent in parallel. That is, up to 20% of the
messages for each destination should be sent at the provisioned pacing rate.

Note: if the node receives an RSR/RCR message for a destination included in the TFA/TCA
messages which are being paced, the node may either:

- Respond to the RSR/RCR with a TFA/TCA, respectively
- Take no action and allow the pacing of the TFA/TCA message to mark the destination
  allowed.

### 4.2.4.13.2 Requirements Associated with Cluster Management

This subsection considers additional requirements for the transfer-allowed procedure
associated with cluster management. Note that a requirement related to cluster management
also appears in Section 4.2.4.13.1. For an overall description of cluster management, see
Appendix D.

An STP may send a TCA message not only under the conditions described in Sections
4.2.4.13, 4.2.4.13.1 and 4.2.4.13.1B, and in Section 13.3 in T1.111.4 of GR-246-CORE,
but also in cases when it performs full PC rather than cluster routing for a local or remote
cluster. Recall that as discussed in Section 4.2.4.12.3 of this document, if an STP only
performs full PC routing to a cluster and it recognizes that it can not route messages to any
member of that cluster, the STP may send a TCP message; similarly, as discussed in Section
4.2.4.14.2 of this document, if an STP recognizes that it can not use a normal route to any
member of that cluster due to a normal link set failure, it may send a TCR message for the
cluster. (Sending a TCP or TCR message would reduce the quantity of resulting signaling-
route-set-test messages from the nodes to which they were sent.) To reverse the effect of
such TCP or TCR message, the STP will send a TCA message. The functionality of sending
the TCP, TCR, and TCA messages under these circumstances is optional for the STP, i.e.,
the choice is left to the STP supplier.
When an STP receives a TCA message, it marks the cluster status as allowed on the affected cluster route if that status was previously marked restricted or prohibited. If the cluster was already marked allowed, no action is taken. These actions are similar to those taken upon receipt of a TFA message for an individual SP towards which full PC routing is performed. The x-list for the affected route is not changed as indicated in Requirement R4-176 [185].

R4-176 [185] Upon receiving a TCA message about a cluster for which a cluster route set is provisioned, the STP shall not change the status of the x-list members for the affected cluster and route.

R4-177 [186] CRMD Upon receiving a TCA message about a cluster for which a cluster route set is provisioned, the STP shall not change the status of any member for which an associated member route set is provisioned.

Requirement R4-178 [187] applies to cluster routing and management diversity and describes what an STP should do when it receives a TCA message about a cluster for which it has both a cluster route set and a member route set (for a cluster member) provisioned.

R4-178 [187] CRMD If the STP marks the status of a cluster as allowed on a route upon receipt of a TCA message for the affected cluster and route, and the STP recognizes that a member route set is provisioned in the affected cluster, and the member is marked prohibited on the affected route, then the STP should begin (or continue) the signaling-route-set-prohibited-test procedures about the prohibited member. If the member is marked as restricted on the affected route, then the STP should begin the signaling-route-set-restricted-test procedures about the affected member.

R4-179 [188] Upon receiving a TFA message about a destination which is a member of a cluster for which the STP has no cluster route set provisioned, the STP shall change the status of the affected member route to available.

R4-180 [189] CRMD Upon receiving a TFA message about a destination for which a member route set is provisioned, and if an associated cluster route set is also provisioned and the status of the associated cluster route is available, the STP shall change the status of the member route to available. If the status of the associated cluster route is not available, the STP should ignore the TFA message, and notify operations network personnel.

As Sections 4.2.4.12.3 and 4.2.4.14.2 discuss, after an STP broadcasts a TCA regarding a cluster, it must inform adjacent nodes about the members which are not accessible via normal route(s) (in some circumstances, sending these messages may depend on whether or not the supplier option described in Section 4.2.4.12.3 is implemented). The updating of adjacent nodes about the status of these members is necessary because some nodes may not perform cluster routing for SPs in the affected cluster. (For more details on the motivation for these requirements see Appendix D, Section D.5.3.)
Requirement **R4-181 [190]** considers STP actions upon receiving a TFA message for an individual signaling point of a cluster towards which cluster routing is performed.

**R4-181 [190]** When a TFA message is received at an STP and the STP is performing cluster routing for the affected destination, the STP shall take the following actions independent of whether the affected route is the current route or not.

…

- If the cluster is marked allowed on the affected route, the STP shall remove the affected PC from the x-list associated with the affected route if the PC appears on the list. No action shall be taken if the PC does not appear on the list.

…

- If the cluster is *not* marked allowed on the affected route, the STP shall not change the x-list or status of the cluster. The receipt of a TFA message in this case is considered an error condition, and it shall be reported to operations network personnel.

### 4.2.4.13.3 Performance Requirements

The following performance requirements shall apply to an STP for the transfer-allowed procedure:

**R4-182 [191]** An STP shall broadcast a TFA/TCA message to all accessible adjacent SPs within 0.5 seconds of the trigger event that caused the broadcast.

A trigger event may be:

- Link set becomes available
- TFA/TCA or TFR/TCR message is received for a normal route.

When the broadcast of a TFA/TCA is being paced (see Section 4.2.4.13.1), Requirement **R4-182 [191]** applies to the set of messages that should be sent at any given time.

A related STP performance requirement is stated in Section 4.2.4.15.6 for the signaling-route-set-test procedure. It specifies the time within which a TFA/TCA message must be sent in response to a signaling-route-set-test message.

### 4.2.4.14 Transfer-Restricted Procedure

This section considers both TFR and TCR messages. An STP sends a TFR/TCR message to inform adjacent nodes that, if possible, they should avoid sending messages to the specified destination (referred to as the affected or concerned destination) via that STP. A
TFR message is sent when the affected destination is an individual SP, and a TCR message is sent for a cluster of SPs.

**R4-183** [192] An STP shall initiate and perform the transfer-restricted procedure as discussed in Section 13.4 in T1.111.4 of GR-246-CORE. In addition, the STP shall conform to the requirements for the transfer-restricted procedure discussed below.

Several aspects of the description of the transfer-restricted procedure in GR-246-CORE are clarified below:

**R4-184** [193] A TFR/TCR is broadcast or sent via the response method, as defined in GR-246-CORE, when a destination becomes inaccessible via the normal route(s) (there may be two normal routes corresponding to a combined link set), after the expiration of T1.111.4/T11 or appearance of danger of congestion on the lower priority route set, whichever appears first. Timer T1.111.4/T11 is started when the STP begins using a lower priority route to the affected destination. Note, previously, it was indicated that a TFR/TCR was broadcast only when at least one link set corresponding to a normal route is unavailable because of a link set outage. This was recently changed in ANSI T1 standards to indicate that a TFR/TCR should also be sent when a TFP/TCP is received for both normal routes. Thus, this restriction has been removed.

- One of the actions that may be taken by an STP upon receiving a TFR/TCR message is not stated explicitly in Section 13.4 in T1.111.4 of GR-246-CORE although it is indicated in an SDL (the ITU-T [formerly CCITT] Specification and Description Language) diagram (see Section 16 in T1.111.4 of GR-246-CORE). Requirements **R4-185** [194] and **R4-186** [195] describe this action.

**R4-185** [194] When an STP receives a TFR or TCR message and the STP performs full PC routing or cluster routing respectively towards the affected destination, the STP shall mark the status of the affected destination as restricted on the affected route unless it was already marked so, whether that route is the current route or not.

**R4-186** [195] If a TCR message is received regarding a cluster and the STP only performs full PC routing towards members of that cluster, the STP shall mark the status of all members of that cluster (that appear in the MTP routing table) as restricted on the affected route unless they were already marked so, independently of whether the affected route is the current route or not.

Note that if the affected destination is an individual SP and the STP only performs cluster routing towards that destination, the STP shall take the actions as discussed in
Section 4.2.4.14.2. As indicated in that section, an STP may change the status of the route to the affected destination in the x-list associated with the affected cluster and route. *These actions are not discussed in GR-246-CORE.*

- One of the cases when TFR/TCR messages are sent by an STP is in response to a signaling-route-set-test message. This case is not mentioned in Section 13.4 in T1.111.4 of GR-246-CORE, but it is mentioned in Section 13.5 which discusses the signaling-route-set-test procedure.

- When an STP is performing cluster routing to a particular cluster of SPs, a TFR for one of the SPs may be broadcast while the cluster is accessible. A TFR is sent for an SP if the cluster is accessible and the SP was previously inaccessible and then became accessible only via alternate route[s]. Also, a TFR is sent for an SP if the cluster is accessible via the normal route and then the SP becomes accessible only via an alternate route.

- GR-246-CORE assumes one PC per CCS node and does not consider the possibility of an SPCS which is assigned multiple PCs (see Section 4.2.3.1). Requirements **R4-187 [196]**, **R4-188 [197]**, and **R4-189 [198]** apply:

  **R4-187 [196]** An STP may receive a TFR message about a primary or secondary PC assigned to an adjacent SPCS with multiple PCs. The STP should treat each PC as if it were an independent signaling point and hence shall only update the route status of the affected PC.

  **R4-188 [197]** When an adjacent multiple PC SPCS becomes inaccessible via the normal route but remains accessible via alternate route(s), an STP should send a TFR message about both primary and secondary PCs of the SPCS.

  **R4-189 [198]** When sending a TFR/TCR to a multiple PC SPCS, the STP shall use the primary PC of the SPCS as the DPC of the message.

Additional requirements for the transfer-restricted procedure are considered in the subsections below. They consist of requirements that do not appear in GR-246-CORE and those that GR-246-CORE does not address in detail. The additional requirements can be categorized as follows:

- Broadcasting/Response Method TFR/TCR Message
- Sending TFR/TCR Message When a Higher Priority Route But Not the Normal Route Becomes Available
- Cluster Management.

Additional requirements in these categories are discussed in the following subsections.
4.2.4.14.1  Broadcasting/Response Method TFR/TCR Message

Requirements R4-190 [199] and R4-191 [200] clarify when a TFR/TCR message should be broadcast or sent via the response method, based on the destination status definitions in Section 4.2.4.11.1. Section 4.2.4.14.2 presents an exceptional case to the broadcast procedure relating to cluster management.

**R4-190** [199] A TFR/TCR message shall be broadcast when the STP first recognizes that a destination which was previously inaccessible becomes accessible only via the alternate route(s).

**R4-191** [200] A TFR/TCR message shall be broadcast or sent via the response method when the STP first recognizes that a destination is inaccessible via normal route(s) (but an alternate route to the destination is available or restricted). The TFR/TCR is broadcast or sent via the response method after timer T1.111.4/T11 expires or danger of congestion occurs after the STP begins using the lower priority route to the affected destination.

As stated in GR-246-CORE, a TFR/TCR message is broadcast or sent via the response method to all accessible adjacent nodes except to an adjacent STP via which traffic is routed to the affected destination (a preventive TFP/TCP is sent to that STP as discussed in Section 4.2.4.12.2), except adjacent STP(s) via which traffic was routed to the affected destination prior to the failure(s) causing the TFR/TCR, and except the affected destination (when it is adjacent).

As stated in GR-246-CORE, a TFR message may optionally be broadcast if TFRs are received for equal priority routes (i.e., the equal priority routes are restricted) and the destination is accessible and not restricted.

The following subsections address three topics:

- A TFR/TCR broadcast when a normal link set becomes available
- Pacing the broadcast of TFR/TCR messages
- Sending TFR/TCR Messages by Response Method.

**A. Broadcast of TFR/TCR Message When a Normal Link Set Becomes Available**

As discussed in Section 4.2.4.13.1A, in some cases a TFR/TCR message rather than a TFA/TCA may be broadcast when a normal (combined) link set becomes available. The purpose of broadcasting a TFR/TCR instead of TFA/TCA is to minimize the likelihood of congestion when the first link or first few links in a (combined) link set with 3 or more links become available. Although this topic is discussed in the current issue of GR-246-CORE (see Sections 13.4.2 and 13.4.2A in T1.111.4), GR-246-CORE does not state specific criteria under which an STP broadcasts a TFR/TCR rather than a TFA/TCA. Such specific criteria for a Bcc network are considered below.
For A/E-link sets with three or more links and B/D-combined link sets with three or more links, when a previously unavailable normal (combined) link set becomes available, the STP shall consider the routes corresponding to that (combined) link set restricted while the number of available links in the (combined) link set is less than the minimum number of links considered to be adequate. The minimum number of links considered adequate shall be provisionable on a per-(combined)-link set basis as discussed in a requirement in Section 4.2.4.13.1A. If the routes corresponding to the newly available normal (combined) link set are considered restricted according to the above criterion, the STP shall broadcast TFR/TCR messages regarding previously inaccessible destinations that became accessible at the time of link set restoration.

Note that when the number of available links in the (combined) link set is equal to or exceeds the provisioned minimum number, the normal routes corresponding to this (combined) link set shall be considered available (unless the destinations are marked prohibited or restricted over normal routes corresponding to this [combined] link set), even if the number of available links later falls below the provisioned minimum. However, the danger of congestion criterion discussed in item (2) of Section 13.4.2 in T1.111.4 of GR-246-CORE may apply.

B. Pacing the Broadcast of TFR/TCR messages

In the past, when a destination which was previously accessible became accessible only via alternate route(s) due to a failure of a normal link set, it was assumed that TFR/TCR messages about the destination could be broadcast at once. However, a nearly simultaneous broadcast of all TFR/TCR messages may lead to congestion because the nodes receiving TFR/TCR messages will perform controlled rerouting nearly simultaneously. During the controlled rerouting procedure, messages will be stored in buffers (for T1.111.4/T6) at adjacent SPs and may be released nearly at once by the adjacent SPs for transmission over the alternate route. To address this problem, the T1S1.3 standards working group has introduced an option to regulate the rate of TFR/TCR broadcasts. Although this is stated as an option in GR-246-CORE, the pacing of TFR/TCR messages during broadcast, and the specific method of pacing discussed below, are required in a Bcc network for A/E-link sets and are a supplier option for combined B/D-link sets when the TFR/TCR is broadcast.

Note, GR-246-CORE was updated to allow response method TFRs in this case. Therefore, Requirement R4-193 [202] and Objective O4-194 [203] to pace the TFR/TCRs only apply if the broadcast method is used.

R4-193 [202] When an A/E-link set corresponding to a normal route experiences a failure and T1.111.4/T11 expires (note that this pacing requirement does not apply if congestion on an alternate route is encountered before T1.111.4/T11 expires), and a destination that was previously accessible becomes accessible only via an alternate route(s), the STP shall pace the broadcast of TFR/TCR messages. The rate of broadcast shall be as follows:
… • Up to 20% of the total number of TFRs/TCRs for a destination shall be sent at the expiration of T1.111.4/T11.

… • The subsequent TFRs/TCRs shall be sent in groups of up to 20% of the total number of TFRs/TCRs for a destination at the provisioned pacing rate, unless the current alternate route encounters a danger of congestion, in which case the remaining TFRs/TCRs shall be sent immediately. The pacing rate shall be provisionable in increments of 0.1 seconds, with a range of 0 to 1 seconds, and a default of 1 second. If the value is set to 0, no pacing shall be done (i.e., the TFR/TCR shall be broadcast without any pacing). A single pacing rate shall be provisionable for both TFA/TCA and TFR/TCR broadcasts. For the discussion of pacing of TFA/TCA broadcasts see Section 4.2.4.13.1B.

… • If the destination becomes inaccessible or accessible via the normal route(s) before all of the TFRs/TCRs are generated, then the remaining TFRs/TCRs shall not be generated. The procedures for TFP/TCP or TFA/TCA shall then be followed.

O4-194 [203] It is desirable that Requirement R4-193 [202] for pacing the broadcast of TFR/TCR messages shall also apply when a combined B/D-link set corresponding to a normal route experiences a failure and T1.111.4/T11 expires (note that this pacing requirement does not apply if congestion on an alternate route is encountered before T1.111.4/T11 expires), and a destination that was previously accessible becomes accessible only via the alternate route(s).

C. Sending TFR/TCR Messages By Response Method

For a variety of reasons, e.g., message loss or STP overload, a broadcasted TFR/TCR message may not be acted upon by an adjacent node. Hence, as stated in GR-246-CORE, an STP shall resend a TFR/TCR message once per link or link set after the broadcast.

R4-195 [204] When a TFR/TCR message is broadcast, the STP shall start a timer T1.111.4/T18. If the STP paces sending the TFR/TCR, the timer shall be started after the pacing is complete. If the link set failure is still present after T1.111.4/T18 expires, a TFR/TCR message should be sent once per incoming link or link set in response to the next message received on that link or link set for the restricted destination.

If a TFR/TCR is sent by response method instead of broadcast method (when the normal link set becomes unavailable and T1.111.4/T11 expires, when there is a danger of congestion on the normal link set, or for signaling message handling congestion) the method for sending those TFR/TCRs is described below.
When a TFR/TCR message is sent by the response method, the STP shall send a TFR/TCR once per incoming link or links set in response to messages received for the newly restricted destination. The STP shall start a timer T1.111.4/T18 after the first response method TFR/TCR is sent. While T18 is running TFR/TCR messages are not sent in response to messages received for the affected destination if a TFR/TCR has previously been sent to the adjacent signaling point concerning that destination. If the link set failure or internal capacity reduction is still present after T1.111.4/T18 expires, a TFR/TCR message should be sent once per incoming link or link set in response to the next message received on that link or link set for the restricted destination.

4.2.4.14.2 Requirements Associated With Cluster Management

This subsection considers additional requirements for the transfer-restricted procedure associated with cluster management. For an overall description of cluster management, see Appendix D.

The following items clarify the broadcasting and response method of TCR/TFR messages with regard to cluster management.

- **R4-197** [206] An STP shall broadcast or send response method TFRs about a member which is accessible only via alternate route(s) only if the STP knows that it is an existent member because a member route set is provisioned for the member, or the member becomes accessible only via the alternate route(s) as a result of being placed on, removed from, or remaining on an x-list. In other words, a TFR message is only sent if the STP knows that the affected member is an existent member.

- **R4-198** [207] An STP shall broadcast a TCR message when a previously inaccessible cluster becomes accessible only via the alternate route(s).

- **R4-199** [208] An STP shall broadcast or send via the response method TCRs when a cluster is inaccessible via normal route(s) (but an alternate route to the cluster is available or restricted). The TCR is broadcast or sent via the response method when timer T1.111.4/T11 expires or danger of congestion occurs on the lower priority route. Timer T1.111.4/T11 is started when the STP begins using a lower priority route for the affected destination.

An STP may send a TCR message not only under the conditions described above and in Section 13.2 in T1.111.4 of GR-246-CORE, but also in cases when it performs full PC rather than cluster routing for a local or remote cluster. Specifically, if an STP only performs full PC routing to a cluster of SPs and it recognizes that it can not route messages
to any member of that cluster via the normal routes because of link set unavailability on normal routes, it may send a TCR message for the cluster. This would reduce the quantity of resulting signaling-route-set-test messages from the nodes to which it sends the TCR message. The functionality of sending the TCR message under these circumstances is optional for the STP, i.e., the choice is left to the STP supplier. See also related paragraphs for TCP and TCA messages in Sections 4.2.4.12.3 and 4.2.4.13.2 respectively.

After an STP broadcasts or sends TCR messages via the response method, it must inform its adjacent nodes about the inaccessible cluster members by sending TFP messages (under certain circumstances, sending TFP messages may depend on the implementation of the supplier option described in Section 4.2.4.12.3). This is given in a requirement in Section 4.2.4.12.3. The motivation for this requirement is described in Appendix D, Section D.5.3.

Requirement R4-199 [208] explains the actions taken by the STP when the STP broadcasts a TCA message about a cluster and there exists members of the affected cluster which are accessible only via the alternate route(s). (There is a similar requirement for inaccessible members in Section 4.2.4.12.3.)

R4-200 [209] If an STP sends a TCA message concerning a remote cluster to an adjacent node and some members of that cluster are accessible only via the alternate route(s), the STP shall be able to inform the adjacent node of these members, in one of the following two ways:

... • It shall send a TFR message for each member that is accessible only via the alternate route(s) after each TCA message is sent to the adjacent node, immediately after any TFP messages are sent for inaccessible members (as discussed in Section 4.2.4.12.3).

... • It shall start or restart any running T1.111.4/T18 timers for these members (i.e., the members accessible only via the alternate route[s]) of the cluster, if any, and be able to send response method TFR messages immediately after the broadcast of the TCA message. In the response method a TFR message is sent once per link or link set in response to the first message received on that link or link set for the member which is accessible only via the alternate route while T18 is running. After T1.111.4/T18 expires, TFRs are again sent once per incoming link or link set in response to messages destined to the affected member.

When an STP receives a TCR message, it changes the status of the cluster route to restricted on the affected cluster route if the cluster was previously marked prohibited or allowed. If the status of the cluster route was already marked restricted when the TCR message for that cluster was received for the affected route, no action is taken. These actions are similar to those taken upon receipt of a TFR message for an individual SP towards which full PC routing is performed.
If an STP changes the cluster route status to restricted upon receipt of a TCR message, the
STP may either remove restricted members from the x-list associated with the affected
cluster and route, or it may leave the x-list unchanged. The choice of whether to keep or
remove restricted members from the x-list is left to the STP supplier. The argument for
keeping restricted members on the x-list is that their status will not change while the cluster
route is restricted because the status of the cluster route will change as soon as the first
member of the cluster becomes accessible via the direct link set at the adjacent STP sending
the TCR message.

Requirement **R4-201** \[210\] considers STP actions upon receiving a TFR message for an
individual SP towards which cluster routing is performed.

**R4-201** \[210\] When a TFR message is received at an STP and the STP is
performing cluster routing for the affected destination, the STP shall
perform the following actions independent of whether the affected route is
the current route or not.

... • If the cluster is marked allowed on the affected route, the STP shall add
the restricted PC to the x-list if the PC was not already listed. If the
affected PC was already listed as restricted on the affected route, no
action shall be taken. If the affected PC was already listed as
prohibited on the affected route, the prohibited status shall be updated
to restricted.

... • If the cluster is marked restricted on the affected route and the affected
PC is listed as restricted in the x-list, no action shall be taken. If the
affected PC is not listed, no action shall be taken. If the affected PC is
listed as prohibited, the affected PC should be removed from the x-list
or its status should be changed to restricted.

... • If the cluster is marked prohibited on the affected route, the STP shall
not change the x-list or status of the cluster. The receipt of a TFR
message in this case is considered an error condition, and it shall be
reported to operations network personnel.

**4.2.4.14.3 Additional Requirements Associated with Cluster Routing and
Management Diversity**

Requirement **R4-202** \[211\] applies if both member route sets and a cluster route set are
provisioned in a cluster. The failure scenario it applies to is the case when a member for
which a member route set is provisioned is accessible via normal route(s), but the cluster
route set shows that the cluster is inaccessible via the normal route(s). An example is if an
STP has available E-links for one member, but one B-link set toward the cluster is
unavailable and the cluster is marked prohibited on the route corresponding to the other B-
link set.
R4-202  [211] CRMD If a message addressed to a particular destination $a$ is received and the following four conditions apply:

... 1. The STP does not have a member route set provisioned for $a$

... 2. The STP has a member route set provisioned for a different member of the same cluster as $a$, and the member route set shows the status of that member to be accessible via a normal route

... 3. The STP has a cluster route set provisioned for the cluster of which $a$ is a member

... 4. Member $a$ is accessible only via alternate route(s).

Then, after the expiration of $T_{11}$ or danger of congestion on the alternate route(s), the STP should send a TFR message in response to the first received message destined to member $a$, once per link or link set.

Requirements R4-203 [212], R4-204 [213], and R4-205 [214] apply when a TCR message is received about a cluster which has a cluster route set provisioned, and a member route set for a cluster member is also provisioned.

R4-203  [212] CRMD When a TCR is received at an STP and a member route set is provisioned in the cluster (i.e., an associated member route set is provisioned), then, if the affected route is in the member route set and the member is marked allowed on the route, the STP shall change the status of the member to restricted on the route. If the member is marked prohibited on the route, the status is not changed upon receipt of the TCR message.

R4-204  [213] CRMD If the STP changes the status of a cluster route from prohibited to restricted upon receipt of a TCR message, a member route set is provisioned in the affected cluster, and the affected member route is prohibited, then the STP should begin (or continue) the signaling-route-set-test procedures about the affected member.

R4-205  [214] CRMD When a TFR about a destination is received at an STP and the STP recognizes that a member route set is provisioned for the member, then, if the affected route is in the cluster route set and the associated cluster route status is either allowed or restricted, the STP should change the status of the member route to restricted. The STP shall also begin (or continue) signaling-route-set-test procedures if the status of the cluster route is allowed. If the associated cluster route status is prohibited, then the STP should ignore the TFR message, and notify operations network personnel.
4.2.4.14.4 Performance Requirements

Requirements R4-206 [215] and R4-207 [216] apply to an STP for the transfer-restricted procedure:

R4-206 [215] An STP shall send a TFR/TCR by the response method within 0.5 seconds of the time the STP first recognizes that a previously isolated destination PC becomes accessible.

R4-207 [216] An STP shall send a TFR/TCR by the broadcast method to all accessible adjacent SPs within 0.5 seconds of the time the STP first recognizes that a previously isolated destination PC becomes accessible.

4.2.4.15 Signaling-Route-Set-Test Procedure

A signaling-route-set-test message is sent by an STP to an adjacent STP to test whether messages to a particular destination or cluster may be routed via that STP.

R4-208 [217] An STP shall initiate and perform the signaling-route-set-test procedure as discussed in Section 13.5 in T1.111.4 of GR-246-CORE unless indicated otherwise in requirements in this section. The STP shall also conform to additional requirements for the signaling-route-set-test procedure discussed below.

R4-209 [218] GR-246-CORE assumes one PC per CCS node and does not consider the possibility of an SPCS which is assigned multiple PCs (see Section 4.2.3.1). Such an SPCS is required to use its primary PC as the OPC in a signaling-route-set-test message. (Recall that at an STP, the primary PC of the SPCS is provisioned as the far end PC of the link set connecting the STP and SPCS.) Thus an STP shall not accept a signaling-route-set-test message when the OPC in the message is a secondary PC of the SPCS.

The term tested destination will be used below to refer to the destination specified in the signaling-route-set-test message the accessibility of which is being tested.

The term equally or less (more) restrictive condition will be used below when the routing status of a cluster member is compared to the routing status of the cluster. Prohibited status is considered more restrictive than the restricted status, and the latter is more restrictive than the allowed status.

Several aspects of the description of the signaling-route-set-test procedure in GR-246-CORE are clarified below:
• Note that if the tested destination is an individual SP and the STP receiving the signaling-route-set-test message performs cluster routing towards that destination, the STP shall take the actions discussed in Section 4.2.4.15.3. These actions are not discussed in GR-246-CORE.

• There are several types of signaling-route-set-test messages that are distinguished by the “signaling-route-set-test signal” parameter:
  — Signaling-route-set-test-prohibited (RSP message, sent upon receipt of a TFP)
  — Signaling-route-set-test-restricted (RSR message, sent upon receipt of a TFR)
  — Cluster-signaling-route-set-test-prohibited (RCP message, sent upon receipt of a TCP)
  — Cluster-signaling-route-set-test-restricted (RCR message, sent upon receipt of a TCR).

A particular type of signaling-route-set-test message is sent until the condition being tested - prohibited, restricted, cluster-prohibited, or cluster-restricted - changes to another condition for the tested destination and route, or, if the tested destination is an individual SP, an equally or more restrictive routing status is reported (in a TCx message) for the cluster of which the tested destination is a member. GR-246-CORE does not explicitly mention that an STP must stop sending a signaling-route-set-test message in the latter case (see Section 4.2.4.15.3 for more information).

A summary of events causing a stop in sending of a particular type of signaling-route-set-test message is presented in Section 4.2.4.15.5.

Additional requirements for the signaling-route-set-test procedure can be categorized as follows:

• Different Timer for Routes of Lower Priority Than the Current Route
• Deactivation of Signaling-Route-Set-Test
• Cluster Management
• Requirements Associated with Additional Criteria for Sending Preventive TFP/TCP Messages
• Performance Requirements.

Additional requirements in these categories are discussed in the following subsections. A summary of requirements for sending and responding to a signaling-route-set-test message is presented in the last subsection.

In the subsequent subsections, RCx is used to indicate cluster-signaling-route-set-test-prohibited or -restricted messages and RSx is used to indicate signaling-route-set-test-prohibited or -restricted messages.
4.2.4.15.1 Different Timer for Routes of Lower Priority than the Current Route

If the route to be tested is of lower priority than the current route to the tested destination, STP resources can be saved if the STP were to send signaling-route-set-test messages less frequently than for the tested route of higher or equal priority to the current route (i.e., less frequently than the timer T1.111.4/T10). The following conditional requirement considers the possibility of sending signaling-route-set-test messages less frequently for routes of lower priority than the current route or even not at all.

CR4-210 [219] As a per-Bcc option, it shall be possible to provision a timer specifying how frequently signaling-route-set-test messages shall be sent for routes of lower priority than the current route. The timer shall be provisionable on an STP-basis, i.e., it shall not depend on the affected destination or cluster. It shall also be possible to suspend sending of signaling-route-set-test messages for routes of lower priority than the current route. However, if the route being tested or for which the test has been suspended is needed to route messages to their destinations, the time between the tests returns to the value of T1.111.4/T10.

4.2.4.15.2 Deactivation of Signaling-Route-Set-Test

Signaling-route-set-test messages may sometimes be sent for a non-existent destination. As Requirement R4-211 [220] discusses, manual intervention may then be needed to make an STP stop sending such messages. It should be noted that the second and the third bullet items of the Requirement R4-211 [220] apply only if cluster routing diversity is provisioned for the concerned cluster.

R4-211 [220] It shall be possible to manually deactivate any signaling-route-set-test and perform one of the following actions:

…

• If the tested destination is an individual SP of a cluster for which a cluster route set is provisioned and no member route set is provisioned for the tested destination, the STP shall remove the status record of the tested destination from the x-list pertaining to that cluster route

…

• In the case of cluster routing and management diversity, if the tested destination is an individual SP for which a member route set is provisioned and the tested member route has an associated cluster route, then the status of the destination on that route is updated to the status of the cluster on the associated cluster route

…

• In the case of cluster routing and management diversity, if the tested destination is an individual SP for which a member route set is provisioned and the tested member route does not have an associated
cluster route, then the status of the destination on that route is updated to the overall status of the cluster from the STP’s perspective

... • If the destination is a member of a cluster for which the STP performs full PC routing, the status of the tested destination on that route is changed to allowed

... • If the tested destination is a cluster, then the status of the cluster on that route is changed to allowed.

4.2.4.15.3 Overview of Requirements Associated with Cluster Management

This subsection presents an overview of additional requirements associated with cluster management for the signaling-route-set-test procedure. The requirements themselves appear in Section 4.2.4.15.5 which summarizes all requirements related to sending and responding to a signaling-route-set-test message.

When the tested destination is an individual SP towards which cluster routing is performed, an STP must stop sending the signaling-route-set-test (RSx) message when the status of the cluster, of which the tested destination is a member, changes (upon receipt of a TCx message) to an equally or more restrictive condition on the same route.

When the tested destination is an individual SP for which only full PC routing is performed, an STP must stop sending the signaling-route-set-test (RSx) message when, upon receipt of a TCA message, the status of the cluster of which the tested destination is a member changes to allowed on the same route (because the routing status of the cluster is assigned to the tested destination).

When the STP receives TCR or TCP message regarding a cluster of signaling points towards which only full PC routing is performed, the signaling points are marked as restricted or prohibited, respectively, on the affected route and the RCR or an RCP procedures, respectively, are started for the affected cluster. As a supplier option, the RSR or RSP procedures, respectively, could be started for each member of the cluster on the affected route as well.

When the tested destination specified in a received signaling-route-set-test (RSx) message is an individual SP towards which cluster routing is performed, an STP must respond with an appropriate TFx message regarding the tested destination under following conditions:

• If the status of the cluster is less restrictive than the status specified in the received signaling-route-set-test message and the SP is not on the x-list.

• If the status of the cluster is less restrictive than the status specified in the received signaling-route-set-test message and the SP is on the x-list but is also marked with a less restrictive status.
• If the status of the cluster is less restrictive than or equally restrictive to the status specified in the received signaling-route-set-test message and the SP is on the x-list and is marked with a more restrictive status.

• If the statuses of both the cluster and the SP are equally restrictive and the status specified in the received signaling-route-set-test message is more restrictive than the status of the SP.

When the tested destination specified in the received cluster-signaling-route-set-test (RCx) message is a local cluster, an STP must respond with a TCA message regarding that cluster (unless the STP happens to send TCR and TCP messages for a local cluster, which is a function left as a supplier option, as discussed in Sections 4.2.4.12.3 and 4.2.4.14.2).

### 4.2.4.15.4 Overview of Requirements Associated with Additional Criteria for Sending Preventive TFP/TCP Messages

As discussed in Appendix A, additional criteria for sending preventive TFP/TCP was introduced to avoid circular routing in the presence of E-links or complex network architectures. GR-246-CORE does not address in detail the impact of these criteria on the signaling-route-set-test procedure, and hence it is considered here. Only an overview of additional requirements is presented - the requirements themselves appear in Section 4.2.4.15.5 which summarizes all requirements related to sending and responding to a signaling-route-set-test message.

When a signaling-route-set-(cluster)-prohibited-test (RSP or RCP) message is received from an adjacent STP to which a preventive TFP/TCP regarding the tested destination or cluster, of which the tested destination is a member, was sent (and was not followed by a TFR/TCR or TFA/TCA), the STP shall take no action.

When a signaling-route-set-(cluster)-restricted-test (RSR or RCR) message is received from an adjacent STP to which a preventive TFP/TCP regarding the tested destination or cluster, of which the tested destination is a member, was sent (and was not followed by a TFR/TCR or TFA/TCA), the STP shall send a TFP/TCP message regarding the tested destination to that adjacent STP.

### 4.2.4.15.5 Summary of Rules for Sending and Responding to Signaling-Route-Set-Test Message

This section summarizes the rules for sending a signaling-route-set-test message. A signaling-route-set-test message is sent every T1.111.4/T10, unless a different timer is used for a route of lower priority than the current route as discussed in a conditional requirement in Section 4.2.4.15.1. In this section, a dagger (†) denotes a feature not addressed or not addressed in detail in GR-246-CORE.
R4-212 [221] When a destination is marked prohibited on a particular route upon receipt of a TFP message, an STP shall periodically send a signaling-route-set-prohibited-test (RSP) message to the sender of the TFP message until any of the following messages are received from the sender (over a direct link set or via another STP):

... • A TFA message for the affected SP
... • A TFR message for the affected SP
... • A TCP message for the cluster of which the affected SP is a member†
... • A TCR message for the cluster of which the affected SP is a member and the STP performs full PC routing towards the cluster
... • A TCA message for the cluster of which the affected SP is a member and the STP performs full PC routing towards the cluster.

R4-213 [222] If the STP receives a TCA or TCR message for a cluster that is marked prohibited on the affected route and there are prohibited members on the x-list associated with the affected cluster and route (maintaining prohibited cluster members on the x-list while the cluster itself is prohibited is a supplier option, as discussed in Section 4.2.4.12.3), then the STP shall immediately resume periodic sending of signaling-route-set-prohibited-test (RSP) messages for each prohibited cluster member until a TFA or a TFR message about the member or a TCP message about the cluster is received.

R4-214 [223] CRMD If the STP receives a TCA or TCR message for a cluster that is marked prohibited on the affected route and there is an associated member route set provisioned, indicating the member is prohibited, then the STP shall immediately resume periodic sending of signaling-route-set-prohibited-test (RSP) messages for each prohibited cluster member until a TFA or a TFR message about the member or a TCP message about the cluster is received.

R4-215 [224] When a destination is marked restricted on a particular route upon receipt of a TFR message, an STP shall periodically send a signaling-route-set-restricted-test (RSR) message to the sender of the TFR message until any of the following messages are received from the sender (over a direct link set or via another STP):

... • A TFA message for the affected SP.
... • A TFP message for the affected SP.
... • A TCP message for the cluster of which the tested destination is a member.†
… • A TCR message for the cluster of which the tested destination is a member.

… • A TCA message for the cluster of which the tested destination is a member and the STP performs full PC routing towards the cluster.

R4-216  [225] If the STP receives a TCA message for a cluster that is marked restricted and there are restricted members on the x-list associated with the affected cluster and route (maintaining restricted cluster members on the x-list while the cluster itself is restricted is a supplier option, as discussed in Section 4.2.4.14.2), then the STP shall immediately resume periodic sending of signaling-route-set-restricted-test (RSR) messages for each restricted cluster member on that route until a TFA or a TFP message about the member, or a TCP or a TCR message about the cluster is received.

R4-217  [226] CRMD If the STP receives a TCA message for a cluster that is marked restricted on the affected route and there is an associated member route set provisioned, indicating the member is restricted on the same route then the STP shall immediately resume periodic sending of signaling-route-set-restricted-test (RSR) messages for each restricted cluster member on that route until a TFA or a TFP message about the member, or a TCP or a TCR message about the cluster is received.

R4-218  [227] When a destination is marked prohibited on a particular route upon receipt of a TCP message, an STP shall periodically send a cluster-signaling-route-set-prohibited-test (RCP) message to the sender of the TCP message until any of the following messages are received from the sender (over a direct link set or via another STP):

… • A TCA message for the affected cluster

… • A TCR message for the affected cluster.

As a non-preferred option, upon receiving a TCP message the STP may send signaling-route-set-prohibited-test (RSP) messages for each member of the affected cluster for which the STP is performing full point code routing and uses the affected route. The conditions under which the STP should subsequently stop sending such messages are identical to the conditions that would apply if the STP received a TFP message for each member of the cluster.

R4-219  [228] When a destination is marked restricted on a particular route upon receipt of a TCR message, an STP shall periodically send a cluster-signaling-route-set-restricted-test (RCR) message to the sender of the TCR message until any of the following messages are received from the sender (over a direct link set or via another STP):
… • A TCA message for the affected cluster
… • A TCP message for the affected cluster.

As a non-preferred option, upon receiving a TCR message the STP may send signaling-route-set-restricted-test (RSR) messages for each member of the affected cluster for which the STP is performing full point code routing and uses the affected route. The conditions under which the STP should subsequently stop sending such messages are identical to the conditions that would apply if the STP received a TFR message for each member of the cluster.

Two general rules for responding to a signaling-route-set-test (RSx or RCx) message are as follows:

1. An STP should not respond to a signaling-route-set-test message if the routing status of the tested destination is the same as that specified in the received message; if the two statuses differ, the TFx/TCx message sent to the sender of the signaling-route-set-test message will depend on the received message. If a (cluster)-signaling-route-set-prohibited-test (RSP/RCP) message is received from an adjacent STP to which a preventive TFP/TCP regarding the tested destination or cluster, of which the tested destination is a member, was sent (and was not followed by a TFR/TCR or TFA/TCA), then the STP shall not respond to the test message.

2. When an STP receives a RSx message, it must respond with a TFx message except under certain circumstances (described in the requirement below) when it should not send a message in response. When an STP receives a RCx message, it must respond with a TCx message except under certain circumstances (described in the requirement below) when it should not send a message in response.

The exact rules for responding to a signaling-route-set-test message are summarized in Requirement R4-220 [229]. The term restricted for the tested destination is used to describe the overall status of that destination as follows: The tested destination is restricted if T1.111.4/T11 has expired.

**R4-220** [229] An STP shall take the actions described below upon receiving a particular type of signaling-route-set-test message:

… • Received signaling-route-set-prohibited-test (RSP) message:

… — No action is taken if the tested destination is inaccessible, or if there is no entry corresponding to the tested destination or to the cluster, of which the tested destination is a member, in the MTP routing table.†

… — No action is taken if the signaling-route-set-prohibited-test message is received from an adjacent STP to which a preventive TFP/TCP message regarding the tested destination or cluster, of which the tested destination is a member, was sent.
... — A TFR message regarding the tested destination is sent if the tested destination is restricted or a normal route to the tested destination or cluster (of which the tested destination is a member) is in danger of congestion, and the sender of the signaling-route-set-prohibited-test message is *not* an adjacent STP to which a preventive TFP/TCP message regarding the tested destination or cluster (of which the tested destination is a member) was sent.†

... — Except for a case considered in the next paragraph, a TFA message regarding the tested destination is sent if the tested destination is allowed in accordance with the status definitions in Section 4.2.4.11.1, and the sender of the signaling-route-set-prohibited-test message is *not* an adjacent STP to which a preventive TFP/TCP message regarding the tested destination or cluster, of which the tested destination is a member, was sent.†

... As discussed in Sections 4.2.4.13.1A and 4.2.4.14.1B, when a (combined) link set with 3 or more links becomes available, the STP shall consider the normal routes corresponding to that (combined) link set restricted while the number of available links in the (combined) link set is less than the minimum number of links considered to be adequate. Thus, if under those circumstances the tested destination is considered restricted, a TFR message will be sent instead of a TFA message discussed in the paragraph above.

... • Received signaling-route-set-restricted-test (RSR) message:

... — No action is taken if the status of the tested destination or of the cluster, of which the tested destination is a member, is restricted.

... — A TFP message regarding the tested destination is sent if the tested destination is inaccessible, or if there is no entry corresponding to the tested destination or to the cluster, of which the tested destination is a member, in the MTP routing table.†

... — A TFP message regarding the tested destination is sent if the signaling-route-set-restricted-test message is received from an adjacent STP to which a preventive TFP/TCP message regarding the tested destination or cluster, of which the tested destination is a member, was sent.

... — Except for a case considered in the next paragraph, a TFA message regarding the tested destination is sent if the tested destination is accessible via normal route(s) in accordance with the status definitions in Section 4.2.4.11.3, and the sender of the signaling-route-set-restricted-test message is *not* an adjacent STP to which a
preventive TFP/TCP message regarding the tested destination or cluster, of which the tested destination is a member, was sent.†

As discussed in Sections 4.2.4.13.1A and 4.2.4.14.1B, when a (combined) link set with 3 or more links becomes available, the STP shall consider the normal routes corresponding to that (combined) link set restricted while the number of available links in the (combined) link set is less than the minimum number of links considered to be adequate. Thus, if under those circumstances the tested destination is considered restricted, no action is taken.

— If the node that receives the RSR message is pacing the broadcast of TFA/TCA messages and the pacing of broadcast TFA/TCA messages includes the destination tested by the RSR message, the STP may either:

— respond to the RSR with a TFA

— take no action and allow the pacing of the TFA/TCA message to mark the destination allowed.

• Received cluster-signaling-route-set-prohibited-test (RCP) message:

— No action is taken if the tested destination is inaccessible, or if there is no entry corresponding to the cluster or a cluster member in the MTP routing table.†

— No action is taken if the cluster-signaling-route-set-prohibited-test message is received from an adjacent STP to which a preventive TCP message regarding the tested destination was sent.†

— A TCR message regarding the tested cluster is sent if the tested cluster is restricted or a normal route to the tested cluster is in danger of congestion, and the sender of the cluster-signaling-route-set-prohibited-test message is not an adjacent STP to which a preventive TCP message regarding the tested cluster was sent.†

— Except for a case considered in the next paragraph, a TCA message regarding the tested cluster is sent if the tested cluster is accessible via normal route(s) in accordance with the status definitions in Section 4.2.4.11.1, and the sender of the cluster-signaling-route-set-prohibited-test message is not an adjacent STP to which a preventive TCP message regarding the tested cluster was sent.

As discussed in Sections 4.2.4.13.1A and 4.2.4.14.1B, when a (combined) link set with 3 or more links becomes available, the STP shall consider the normal routes corresponding to that
(combined) link set restricted while the number of available links in the (combined) link set is less than the minimum number of links considered to be adequate. Thus, if under those circumstances the tested cluster is considered restricted, a TCR message will be sent instead of a TCA message discussed in the paragraph above.†

... — When only member route sets are provisioned for the cluster corresponding to the tested cluster in the cluster-signaling-route-set-prohibited-test message,†

... • A TCA message regarding the tested cluster is sent if the supplier option of sending TCR message (discussed in Section 4.2.4.14.2) is not implemented, or if it is implemented but at least one member of the tested cluster is accessible via the normal route.

... • A TCR message regarding the tested cluster is sent if the supplier option discussed in Section 4.2.4.14.2 is implemented and at least one member is accessible via an alternate route and no member is accessible via a normal route.

... • Received cluster-signaling-route-set-restricted-test (RCR) message:

... — No action is taken if the status of the tested cluster is restricted.

... — A TCP message regarding the tested cluster is sent if the tested cluster is inaccessible, or if there is no entry corresponding to the cluster or a cluster member in the MTP routing table.†

... — A TCP message regarding the tested cluster is sent if the cluster-signaling-route-set-restricted-test message is received from an adjacent STP to which a preventive TCP message regarding the tested cluster was sent.†

... — Except for a case considered in the next paragraph, a TCA message regarding the tested cluster is sent if the tested cluster is allowed in accordance with the status definitions in Section 4.2.4.11, and the sender of the cluster-signaling-route-set-restricted-test message is not an adjacent STP to which a preventive TCP message regarding the tested cluster was sent.

... As discussed in Sections 4.2.4.13.1A and 4.2.4.14.1B, when a (combined) link set with 3 or more links becomes available, the STP shall consider the normal routes corresponding to that (combined) link set restricted while the number of available links in the (combined) link set is less than the minimum number of
links considered to be adequate. Thus, if under those circumstances the tested cluster is considered restricted, a TCA message is not sent.†

... — If the node that receives the RSR message is pacing the broadcast of TFA/TCA messages and the pacing of broadcast TFA/TCA messages includes the destination tested by the RSR message, the STP may either:

... — respond to the RSR with a TFA

... — take no action and allow the pacing of the TFA/TCA message to mark the destination allowed.

... — When only member route sets are provisioned for the cluster corresponding to the tested cluster in the cluster-signaling-route-set-restricted-test message,†

... • A TCA message regarding the tested cluster is sent if the supplier option of sending TCP message (discussed in Section 4.2.4.12.3) is not implemented, or if it is implemented but at least one member of the tested cluster is accessible via the normal route.

... • A TCP message regarding the tested cluster is sent if the supplier option discussed in Section 4.2.4.12.3 is implemented and all of the members of the tested cluster are inaccessible.

4.2.4.15.6 Performance Requirements

The following performance requirement shall apply to an STP for the signaling-route-set-test procedure:

R4-221 [230] If an STP must respond to a signaling-route-set-test message with a TFx/TCx message, the TFx/TCx message shall be sent within 0.5 second of the receipt of the signaling-route-set-test message.

4.2.4.16 Transfer-Controlled Procedure

A transfer-controlled (TFC) message is sent by an STP to notify SPs originating message traffic that messages of a given priority or lower should no longer be sent to the specified destination (referred to as the affected destination). It should be noted that no changes to the transfer controlled procedures are necessary to support an SPCS with multiple point codes.
**R4-222** [231] An STP shall initiate and perform the transfer-controlled procedure as discussed in Section 13.7 in T1.111.4 of GR-246-CORE. The STP shall also conform to the additional requirement for the procedure discussed below.

One aspect of the description of the transfer-controlled procedure in GR-246-CORE is clarified below. A TFC message specifies congestion status in routing towards an individual SP. It cannot by design indicate congestion towards a cluster. Thus, when an STP receives a TFC message and the STP performs cluster routing towards the affected destination, the STP cannot determine whether the congestion at the remote STP sending the TFC applies to an individual SP or to the cluster. Therefore, the STP must maintain congestion status of a route set on an individual SP basis, independent of whether it is performing cluster or full PC routing towards the affected SP.

Since GR-246-CORE does not state explicitly that an STP must keep congestion status of a route set on an individual SP basis, this is stated in Requirement **R4-223** [232].

**R4-223** [232] An STP shall maintain congestion status of a route set on an individual SP basis. When a TFC message is received and the STP performs cluster routing for the affected destination, the STP shall mark the route set toward the affected destination as congested with the congestion status carried in the received TFC message. The route set associated with the cluster of which the affected destination is a member shall not be affected by the TFC since congestion is defined on an individual SP basis rather than a cluster basis.

A prompt STP notification of congestion status to signaling end points via TFC messages is desirable to minimize message discard and delay in the network and to maximize message throughput under congestion conditions. The following performance requirement shall apply to an STP for the transfer-controlled procedure:

**R4-224** [233] An STP shall be ready to send a TFC message reporting the appropriate congestion status within 125 ms of exceeding a congestion onset threshold in a link transmit buffer. The 125 ms is considered the 95th percentile; that is 95 percent of the time the sending of TFCs for received messages to the affected link after an onset threshold is exceeded shall occur within 125 ms. The 125 ms criteria shall apply separately to the following two conditions:

a. From the time the congestion onset is triggered at a link to the completion of updating the congestion status of all processors requiring this information

b. From the time a message is received, after the congestion status is updated at the appropriate processors, to placing the TFC in the transmit buffer.
4.2.4.17  Signaling-Route-Set-Congestion-Test Procedure

A signaling-route-set-congestion-test message is sent by a signaling node to request an update of the congestion status associated with the route set between itself and a particular destination point.

R4-225  [234] An STP shall initiate and perform the signaling-route-set-congestion-test procedure as discussed in Section 13.9 in T1.111.4 of GR-246-CORE.

In the past, an STP in a Bcc network had routes of only two priorities to each destination, with the lower priority corresponding to the C-link set. With the introduction of E-links and more complex network architectures, three or more priorities may be possible. Thus, it may be advantageous for an STP to assume that the congestion status of a route set is 0 when it diverts traffic to a route of different priority and that route does not correspond to the C-link set. One of the reasons for assuming a different congestion status is that the rerouted traffic may be reaching a destination through a (combined) E-link set while the previously encountered congestion may have occurred on the (combined) A-link set. The following conditional requirement considers such STP action. (Note that this STP action is not considered in GR-246-CORE.)

CR4-226  [235] As a per-Bcc option, an STP shall set the congestion status of a route set to 0 and stop sending the signaling-route-set-congestion-test messages to a particular SP when it begins routing to that SP via a route of different priority and that route does not correspond to the C-link set.

4.2.4.18  Processing of MTP Network Management Tasks During Processor Overload

This subsection considers STP processing of MTP network management tasks during processor overload, a topic not addressed in GR-246-CORE.

R4-227  [236] The MTP network management processing function shall be designed in such a way that during network management processor overload, processing resources are available on a priority basis for critical (high priority) network management tasks. This capability is referred to as priority processing of network management tasks in this document. A possible description of this capability is summarized below with a detailed discussion provided in Appendix G.

Network management tasks refer to functions provided by the STP processors responsible for performing MTP signaling network management functions required to maintain signaling services and to restore normal signaling operations if disruptions occur in the
signaling links or at SPs. Signaling network management functions are those functions defined in SS7 protocol under the following categories:

- Signaling Traffic Management Functions
- Signaling Route Management Functions
- Signaling Link Management Functions.

Network management tasks under each of the above categories are described in Appendix G.

Priority processing of network management tasks requires the STP to be able to identify all processing tasks associated with a given network management function. The STP should be able to classify these tasks under different priority classes. The priority processing capability is intended to allow the STP to perform higher priority network management tasks before lower priority tasks and thus assure that processing resources are available to perform network management tasks critical to maintaining the integrity of a Bcc CCS network under failure conditions. The network management priority processing capability in the STP is expected to be most valuable when there is a potential for overloading network management processing capacity but as this capability also enhances the general efficiency of the network management task processing, this capability could also remain effective under all conditions. Determination of the specific implementation approach should be based on the design of the STP.

The following additional requirements are considered applicable to support this capability in STPs.

**R4-228** [237] The STP shall be able to identify network management tasks that it should perform in response to received network management messages and for internally generated events due to the detection of local failures (e.g., failures in a link, a link set, the mate STP).

**O4-229** [238] It is desirable that the STP network management tasks are assigned priorities within a range of 0 to 3, with 3 being the highest priority and 0 being the lowest priority.

**O4-230** [239] The task priorities can be based on the following considerations:

...• Priority 3 tasks are those network management tasks that minimize the potential for message loss by providing a path for the message traffic during failures in the network. For example, this includes restoring traffic to a previously inaccessible destination or sending notification via the response method about the inaccessibility of a destination to the adjacent node.
… • Priority 2 tasks are those tasks that enable efficient signaling resource utilization. For example, this includes performing congestion control tasks and restoring traffic to primary routes from alternate routes.

… • Priority 1 tasks are those tasks that prevent escalation of failure effects to other parts of the network. For example, this includes informing adjacent nodes through the broadcast method the status of a destination.

… • Priority 0 tasks are those tasks that are required for surveillance of the CCS networks. For example, this includes sending signaling-route-set-test messages.

O4-231 [240] Specific assignments of priorities to network management tasks should be based on the network management processing principles used in an STP. Appendix G provides guidelines for assignment of priorities to various network management tasks.

R4-232 [241] The priority processing capability shall enable the STP to perform higher priority network management tasks before lower priority tasks.

R4-233 [242] The STP shall assure that prioritized processing of network management tasks does not result in incorrect routing configurations. For example, if a TFP is received followed by a TFR on a route for a destination, the final status of the route should be considered restricted for the affected point code.

O4-234 [243] A task may be discarded after it has been queued in the priority buffer for 1 minute.

CR4-235 [244] If network management tasks are prioritized only during MTP network management processor overload, the following shall apply:

… • The overload of the MTP network management processor shall be determined by the percent processor occupancy.

… • The supplier shall determine the threshold level of the processor occupancy at which the processing would be at risk. The processing risk may comprise a processing delay that may result in not meeting the STP performance requirements specified in Section 4.

… • Once the network management processor occupancy threshold is reached, the STP shall initiate priority processing of its network management tasks.
4.2.5  Signaling Link Tests

R4-236  [245] An STP shall be able to perform the signaling link test described in Section 2.2 of T1.111.7 of GR-246-CORE.

GR-246-CORE assumes one PC per CCS node and does not consider the possibility of an SPCS which is assigned multiple PCs (see Section 4.2.3.1). Such SPCS is required to use its primary PC as the OPC in messages associated with the signaling link test. (Recall that at an STP, the primary PC of the SPCS is provisioned as the far end PC of the link set connecting the STP and SPCS.) Thus an STP shall not accept messages associated with the signaling link test when the OPC in the message is a secondary PC of the SPCS. In addition, when sending messages associated with the signaling link test to a multiple PC SPCS, the STP shall use the primary PC of the SPCS as the DPC of the messages. In addition to the requirements for the signaling link test procedures described in GR-246-CORE, Requirements R4-237 [246] and R4-238 [247] apply.

R4-237  [246] An STP shall:

… • Initiate the signaling link test during link activation/restoration
… • Provide the capability to initiate the signaling link test on demand
… • Provide the capability to run periodic signaling link tests on every available link every T1.111.7/T2 seconds, regardless of whether the link is experiencing transmit or receive congestion. It shall be possible to turn on or off periodic signaling link tests on a per-node basis.

R4-238  [247] The STP shall take a signaling link out of service if a periodic signaling link test fails.

4.2.6  MTP Circular Route Detection

Recently, procedures were added to GR-246-CORE, T1.111.7 Section 2.4 for an MTP circular route detection method. This section gives an overview of those procedures and provides additional details beyond that provided in GR-246-CORE.

4.2.6.1  Trigger for the Circular Route Detection Test

R4-239  [248] As stated in Section 2.4 of T1.111.7 in GR-246-CORE, one of two events, but not both, shall be used by an STP to trigger the execution of the MTP circular route test: either onset of congestion or rerouting of signaling traffic. The choice of which trigger to implement is left to the supplier. Of the two procedures, the congestion trigger mechanism is more effective and thus is preferred. With the routing change trigger, some loops may not
be detected. For example, if a destination is tested after a cluster routing change and is not in a loop, but other destinations in the cluster are involved in a loop, the loop involving the other destinations in the cluster will not be detected.

For the loop test initiated for onset of congestion, the following additions to GR-246-CORE are given:

R4-240 [249] If the link being monitored (i.e., the link in the link set for which congestion onset 1 was exceeded) fails, then the STP shall not initiate the test procedures, but shall monitor the entire link set for an increase in congestion status of any link in the link set. That is, even if the STP had collected and tabulated some messages for the concerned link before it failed, it shall not use this information and the associated procedures shall be canceled.

R4-241 [250] If the congestion status increases on a link which is currently being monitored for the MTP loop detection procedures, but the STP is still collecting the N messages destined for the link for the previous test, then the STP shall not initiate new loop detection procedures for the latter congestion status increase (i.e., N is not reset to 0 and collection procedures are restarted).

GR-246-CORE gives an option of not executing this test on the C-link set. The following guideline is given to determine whether or not the test should be executed on the C-link set.

O4-242 [251] If a (supplier-specific) mechanism exists to ensure MTP routing data consistency between mated STPs, then the circular route test does not need to be performed on the C-link set; otherwise, it is desirable that the test be performed (for the congestion event trigger) on the C-link set.

R4-243 [252] For the routing change trigger, the STP shall not perform the MTP circular route test during the MTP Restart procedures.

4.2.6.2 Procedures for the Circular Route Detection Test

R4-244 [253] Regardless of the event that triggers the test, the STP shall perform the circular route detection test as described in Section 2.4 of T1.111.7 in GR-246-CORE.

Requirements R4-245 [254] and R4-246 [255] provide additional guidelines for the SLS assignment of the test messages.
R4-245  [254] When the congestion test trigger is used, the STP shall assign the SLS code of the test messages such that all STPs that could be used to reach the destination under test could be tested. This may be accomplished, for example, by assigning a randomized SLS code to each test message or by assigning a single SLS code to all test messages for a given test trigger and changing the SLS code for each triggering of the test.

R4-246  [255] When the routing change trigger is used, the STP shall assign the SLS codes with a uniform distribution to the test messages for all destinations (with the exception given below, when a cluster route is being tested after the initial test message is received back at the originating STP).

Requirement R4-247 [256] provides additional guidelines when the trigger event is a routing change and cluster routing or cluster routing diversity is being used.

R4-247  [256] When the test is initiated for a routing change that affects a cluster route set or an associated member route set, the STP shall determine the tested destination as follows:

…  
• For members of the affected cluster with an associated member route set (i.e., when there is cluster routing diversity), a test shall be initiated for each member for which the routing change affects its current routing.

…  
• For members where only cluster routing is used, the STP shall initiate a test for the destination provisioned for testing purposes (the default is 1) for that cluster. If the STP receives the returning test message within $T_{loop}$, the STP shall mark that member prohibited in the x-list on the routes in the route set. In addition, the following actions are a Bcc option.

CR4-248  [257] After the initial test message is received for the cluster, the STP shall send out one test message for every member using the cluster route (i.e., those that do not have associated member route sets and not the initial destination tested) for which messages are received during the next 10 seconds. These messages shall use the same SLS code used by the initial test message. If the STP receives any of the returning priority 3 route-set-congestion-test messages within $T_{loop}$, the individual members, NOT the cluster, shall be marked prohibited on x-list for the routes in the route set. (This is necessary, since the routing error could be at a subsequent node which performs member routing rather than cluster routing.)

GR-246-CORE does not explicitly describe the actions to be performed upon receipt of a test message initiated by the mate STP. These are given below.
R4-249 [258] At any time, if an STP receives a priority 3 route-set-congestion-test message initiated by its mate (received on any link), it shall forward it to the destination indicated in the message.

As indicated in GR-246-CORE, when an STP receives a priority 3 route-set-congestion-test message originated by itself, it should mark the current route set(s) and lower priority routes to the affected destination in the route-set-congestion-test message as prohibited due to MTP loop detection and send transfer-prohibited messages using the response or broadcast method to adjacent signaling points. For a member for which cluster routing applies, this means that the member shall be added to the x-list as prohibited due to MTP loop detection status of all cluster routes. For individual members, each route in the route set shall be marked prohibited due to MTP loop detection. No signaling-route-set-test messages should be sent for the affected routes. To avoid erroneously isolating a signaling point, these actions should only take place if the signaling-route-set-congestion-test message is received within a certain time of the initiation of such a test message, as described below.

R4-250 [259] An STP shall take the actions described in T1.111.7 of GR-246-CORE upon receipt of a route set congestion test message originated by itself only if the message is received for a destination for which it initiated a test within the last $T_{loop}$ seconds.

R4-251 [260] Timer $T_{loop}$ shall be provisionable with a range of 10 - 20 seconds and a default of 10 seconds. If multiple destinations are being tested simultaneously, then timer $T_{loop}$ shall be maintained on a per (combined) link set basis for the congestion trigger and a per rerouting event or provisioning change event for the routing change trigger, and reset when a new test is initiated.

R4-252 [261] If a route set congestion test message is received by the STP that originated that message but $T_{loop}$ is not currently running or the destination is not one for which a loop test was initiated, the STP shall discard the test message and take no further action.

As indicated in GR-246-CORE, when a loop is detected, network operations personnel shall be notified and the current route set(s) and lower priority routes for the affected destination at the STP detecting the loop shall be marked prohibited due to MTP loop detection until network operations personnel or a management system corrects the routing problem and resets the unavailable state, as defined below:

R4-253 [262] The STP shall allow network operations personnel the ability to manually change the status of a destination for each route in a route set to allowed for destinations previously marked prohibited due to detection of an MTP loop. Specifically, when this is requested, the STP shall do the following:
If the requested destination is an individual SP of a cluster for which a cluster route set is provisioned, and no member route set is provisioned for that destination, the STP shall remove the status record of the requested destination from the x-list pertaining to each cluster route in the cluster route set. Thus, the SP assumes the status of the cluster.

In the case of cluster routing and management diversity, if the requested destination is an individual SP for which a member route set is provisioned, and the cluster, of which the destination is a member, is provisioned with a cluster route set, then for each member route which has an associated cluster route, the status of the destination on that route is updated to the status of the cluster on the associated cluster route. For each member route which does not have an associated cluster route, the status of the destination on those routes is updated to the overall status of the cluster from the STP's perspective.

If the destination is a member of a cluster for which the STP performs full PC routing, the status of the requested destination on each route is changed to allowed.

Note, for the routing change trigger, this should be considered a routing status change.

In addition, as indicated in Section 6, maintenance personnel should be reminded every 30 minutes of destinations that remain prohibited due to the detection of an MTP loop.

If the loop involved the use of an erroneous alternate route (this is the most likely case) and a higher priority route is restored, then it would be useful to automatically restart traffic on the recovered route, but leave the lower priority routes prohibited. This would minimize the impact on traffic to the affected destination by restoring traffic while allowing maintenance to continue to track down the error causing the loop.

R4-254 [263] If a higher priority route becomes available, the STP shall send a TFA/TCA or TFR/TCR message, as appropriate. The STP shall not change the status of lower priority routes.

4.3 Signaling Connection Control Part (SCCP)

The SCCP adds specialized routing and management functions to the MTP, e.g., those necessary to provide network routing to replicated databases.

The SCCP provides connection-oriented and connectionless services. Presently, only connectionless services are used in the Bcc networks. SCCP functionality needed for connectionless services at an STP can be grouped into the following functional blocks (see Section 1.4 in T1.112.4 of GR-246-CORE; references to section numbers below are for this document, not GR-246-CORE):
1. **SCCP connectionless control** - this function provides for connectionless transfer of data units (Section 4.3.2)

2. **SCCP management** - this function provides capabilities, in addition to the signaling route management and flow control functions of the MTP, to handle the failure of an SCCP user or the congestion or failure of a signaling route to the SCCP user (Section 4.3.3)

3. **SCCP routing** - upon receipt of a message from the MTP, this function forwards the message to function 1 above, or performs a global title translation (GTT) and/or ISNI (Intermediate Signaling Network Identification - see Appendix E) routing and forwards the message to the MTP for transfer; upon receipt of a message from function 1 above, it forwards the message to the MTP for transfer (Section 4.3.1).

These functions are considered in the subsections below. Section 4.3.4 considers STP processing of SCCP network management tasks during processor overload.

The term **SCCP routing** will be used to refer to both types of routing that an STP may perform - GTT and ISNI.

### 4.3.1 SCCP Addressing and Routing

**R4-255** [264] An STP shall support SCCP addressing as discussed in Section 2.1 of T1.112.4 of GR-246-CORE.

Formats of SCCP parameters, in particular those of SCCP addresses, are described in T1.112.3 of GR-246-CORE. As stated in T1.112.3, two global title formats (a “global title” is an SCCP address which serves as an alias for an MTP address) are possible, corresponding to the values of the global title indicator (a subfield of the address indicator parameter) of 0001 and 0010. As Requirement **R4-256 [265]** indicates, currently an STP in a Bcc network only needs to support the 0010 value. Since the 0001 value is not presently used, an STP does not have to support it at this time.

**R4-256** [265] An STP shall be able to process messages with a global title corresponding to the global title indicator of 0010.

**R4-257** [266] An STP shall perform SCCP routing functions associated with connectionless services as discussed in Sections 2.2, 2.3 and 2.4 of T1.112.4 of GR-246-CORE.

As described in Section 2.4 of T1.112.4 of GR-246-CORE, SCCP message return procedures may be initiated if SCCP routing is unable to transfer a message due to a routing failure. If an SCCP routing failure occurs and the status of the originating node which sent the failed message is available, the STP sends a UDTS/XUDTS message to the originating node indicating the message routing failure. If an SCCP routing failure occurs and the status of the originating node which sent the failed message is prohibited or unknown, the STP
will not send a UDTS/XUDTS message to the originating node. Since subsystem management messages which indicate the status of a subsystem are not supported across network boundaries, an STP may not always be informed of the point code/subsystem status at the originating node.

**R4-258** [267] The STP shall assume the status of a point code or subsystem is available if the status cannot be determined.

For a discussion of the routing of messages containing an SCCP ISNI parameter (note that this parameter is considered in T1.112.3 of GR-246-CORE,) see Appendix E. During the transition period for ISNI, Requirement **R4-259** [268] is needed.

**R4-259** [268] The STP shall provide the operation capabilities described in Sections 6.4.2 and 6.6.2 upon receipt of an unrecognized SCCP message type.

In addition, a return cause to be used when the STP cannot perform ISNI processing, and an XUDTS message will be sent, is described in Section 4.3.1.3. The remaining requirements in this section assume that the STP supports ISNI.

The next subsection provides an overview and requirements for Global Title Translation as it relates to replicated end-nodes/databases. Subsection 4.3.1.2 presents an overview of GTT data at an STP including a description of two-step GTT. The subsections after the GTT data overview discuss additional requirements in the following areas:

- SCCP Hop Counter
- Return Cause Parameter in UDTS and XUDTS Messages
- Verification of XUDT Message Processing Capability.

### 4.3.1.1 Global Title Translation and Endnodes/Databases

Global Title Translation and SCCP management procedures allow network provider to design networks with solitary endnodes/databases or replicated endnodes/databases. The result at an STP doing final Global Title Translation will depend on the number of endnode/database replicates and the mode of operation. This section provides an overview and requirements for Global Title Translation as it relates to endnodes/databases.

#### 4.3.1.1.1 Solitary Node/Subsystem

A node/subsystem that is not replicated is called solitary. This is the simple case when there is a single node/subsystem. Therefore, there is no alternate routing if the node/subsystem fails. The result at an STP doing final Global Title Translation is the address (destination point code/subsystem) of the solitary node/subsystem.
4.3.1.1.2 Multiple Replicates Operating in a Dominant Mode

Prior to describing multiple replicated nodes/subsystems operating in a dominant mode, the following terminology must be introduced:

- **Preferred node/subsystem** - the accessible node/subsystem of highest priority (i.e., lowest relative cost; a node/subsystem currently receiving traffic)

- **Next preferred node/subsystem** - the accessible node/subsystem of next highest priority (i.e., next lowest relative cost) with respect to the preferred node/subsystem (i.e., the node/subsystem that would receive the traffic if the preferred node/subsystem becomes inaccessible)

- **Previously preferred node/subsystem** - the node/subsystem that was previously handling the traffic until another node/subsystem of higher priority (i.e., lower relative cost) became accessible

- **Higher priority node/subsystem** - inaccessible node/subsystem having higher priority (i.e., lower relative cost) than the preferred node/subsystem (i.e., would be preferred if accessible)

In the dominant mode, each replicate of a node/subsystem is associated with a relative cost. The combination of relative cost and accessibility status of the node/subsystem identifies the preferred node/subsystem. At any given time, the preferred node/subsystem is the accessible node/subsystem of lowest relative cost.

In this mode, traffic is split among several nodes/subsystems. Under normal condition, each portion of the traffic is routed to the accessible node/subsystem of lowest relative cost, which is the “preferred node/subsystem”. When the current preferred node/subsystem becomes inaccessible, this traffic is routed to the accessible node/subsystem of next lowest relative cost, or the “next preferred node/subsystem”. Thus, the accessible node/subsystem of next lowest relative cost becomes the preferred node/subsystem. The “previously preferred node/subsystem” refers to the node/subsystem that was previously handling the traffic until either it became inaccessible, or until a lower relative cost node/subsystem becomes accessible. Upon node/subsystem recovery, it becomes the preferred node/subsystem, if it has a lower relative cost than the node/subsystem currently handling the traffic.

Previously, GTT relative cost data item was limited to one of two unique values, as previously described in the ANSI T1 standard and issues of GR-246-CORE prior to Revision 3. This allowed for a single global title (i.e., translation type and global title address combination) to be translated to at most two different destinations (i.e., destination point code and subsystem number), based on relative cost. These were referred to as the primary and backup destinations. The primary destination is given the higher priority (i.e., routing preference) by assigning a lower relative cost value than the relative cost value assigned to the backup.
The ANSI T1 standard was revised to eliminate the limitation of two destination point codes and subsystem numbers per global title. The motivation for eliminating the primary/backup limitation was to provide higher availability of end node databases, even in the presence of multiple, simultaneous failures. Eliminating this limitation allows network providers to equip their networks with three or more replicated databases, as well as with translations that allow automatic rerouting of traffic to an available replicate in case of failure. Previously, if a network is equipped with more than two replicates, translations must be manually changed to reroute traffic if the two provisioned replicates become inaccessible.

A Bcc network may need up to eight destination point codes/subsystem numbers per global title. Thus, Requirement R4-260 [269] applies:

**R4-260 [269]** For any given translation type, an STP shall provide the capability to translate the same global title address to up to 8 different destinations (e.g., destination point code and subsystem number), based on the assignment of 8 unique relative cost values to those destinations.

Note: In the past, with only one primary destination and one backup destination, the STP could determine where (i.e., to which destination) to send the SCCP management messages (i.e., SBR, SNR) in one of two ways. The STP could either use the provisioned GTT data to determine the next preferred or previously preferred destinations based on the relative cost information, or the STP could use the information provisioned in the Mated Application Data (see Section 5.2.3). When there are more than two replicates, the Mated Application Data may no longer be useful for determining which destination should receive traffic and SCCP management messages when the preferred destination becomes inaccessible. The necessary information may be found in the provisioned GTT data. Exactly how this information is used to determine where to send traffic and SCCP management messages is left up to the implementation.

### 4.3.1.1.3 Multiple Replicates Operating in the Loadshare Mode

The ANSI T1 standard allows SCCP load sharing of messages routed on Global Title to replicated nodes/subsystems by assigning equal relative cost values to each replicate. This mode of operation is called the loadshare mode and nodes/subsystems assigned equal cost values are called loadshare nodes/subsystems.

In the loadshare mode, traffic is loadshared among several nodes/subsystems. Under normal conditions the traffic is distributed equally among the available loadshare nodes/subsystems. When a loadshare node/subsystem becomes inaccessible, the traffic is distributed equally among the remaining available loadshare nodes/subsystems. Upon the recovery of an inaccessible loadshare node(s)/subsystem(s), the traffic is redistributed equally among all available loadshare nodes/subsystems.
For a Bcc network, SCCP load sharing of traffic to up to 8 destination point codes/subsystem numbers per global title may be necessary. Thus, the following requirements apply:

**R4-261** [270] For any given translation type, an STP shall provide the capability to translate the same global title address to up to 8 different destinations (e.g., destination point code and subsystem number), based on the assignment of 8 equal cost values to those destinations.

**R4-262** [271] The STP shall provide the capability to loadshare the traffic equally among destinations assigned equal cost values (loadshare nodes/subsystem). The mechanism used to equally distribute the traffic is left up to specific vendors implementation. The vendor specific mechanism shall not prevent load sharing of traffic over available links in a link set (MTP level).

The SCCP load sharing capability does not guarantee load sharing of traffic at the MTP level. Requirements for load sharing of traffic over available links in a (combined) link set are in Section 4.2.3.3 and GR-246-CORE (T1.111.5).

When a loadshare node/subsystem becomes inaccessible the STP shall distribute the traffic equally among the remaining available loadshare nodes/subsystems. Upon the recovery of a loadshare node/subsystem the STP shall redistribute the traffic equally among all available loadshare nodes/subsystems.

As indicated in the requirement above, the load sharing mechanism is left up to the specific vendors implementation. However, vendors should be aware that a segmented message should be kept in sequence and all the segments for a given message should be sent to the same destination (node/subsystem). For example all XUDT segments for the same segmented message should be sent to the same destination.

### 4.3.1.2 Global Title Translation Data

SCCP functions provide for specialized routing based on global titles which include logical addresses rather than physical locations of destination signaling points. Global titles must be translated by STPs to a network address in SS7 format (i.e., in the form of a destination point code) in order for SS7 messages to be routed by MTP functions to the appropriate signaling node destination. In general, a global title is translated to a destination point code and, possibly, a subsystem number, which identifies the application that will process the message. The translation of a global title to a destination point code and subsystem number is referred to as a GTT and is based on GTT data that is provisioned by CCS network personnel.

---

3. Although SCCP at any CCS node may be equipped to perform GTTs, this function is usually performed at the STP.
Global title translation data stored at STPs primarily consists of the following data items: translation type, global title address, destination point code, subsystem number, relative cost, and routing indicator. The translation type identifies the set of GTT data corresponding to a particular application or set of applications, e.g., 800, LIDB, or CLASS, and determines the set of GTT data to be used for the translation. The relative cost indicates the routing preference for a given destination signaling point, where a lower cost corresponds to a higher routing preference toward the destination. The routing indicator determines whether the translation is intermediate or final, i.e., whether a subsequent GTT for the message is required or not. The existing STP GTT user’s view is such that the STP identifies a set of GTT data that is to be used to perform a specific translation function based on the value of the translation type for the SS7 message. As such, the specific set of GTT data that is identified is used to translate the global title address of the SS7 message to a specific destination point code and subsystem number, and associated routing indicator value according to the relative cost value that is provisioned.

One major drawback to the existing STP GTT user’s view is that it may not allow an STP to efficiently use memory space for redundant GTT data and thus requires a large provisioning effort. For example, if the same GTT data is required for two different translation types, CCS network personnel are required to provision GTT data twice (i.e., one set of GTT data for each translation type). Additionally, it is likely that the demand for GTT data memory space will increase further as additional CCS services are introduced, especially for those services that require the same GTT data. As such, the existing GTT user’s view has been revised in order to achieve savings in STP memory space and reduce the GTT data provisioning effort.

To reduce the demand on memory at the STPs, it is expected that the GTT process be performed in several steps. One step in the GTT process would map the translation type to a specific subsystem number. Another step would determine a destination point code based on the global title address that is provisioned. This would allow the consolidation of portions of GTT data when there is significant overlap for different applications (i.e., redundant GTT data). Not only will the demand on STP memory be reduced, but considerable effort in provisioning GTT data can be saved by consolidating identical portions of the data. It is important to note that the existing GTT data structure should continue to be supported at the STP, if desired by a Bcc, to temporarily ease the transition to the multi-step GTT process described above or to permanently retain data provisioned with the existing GTT data structure.

R4-263  [272] For any given translation type, the STP shall provide the capability for “global title address to point code” information to be shared by several translation types.

---

4. In general, a user view describes the data items and the associated relationship between those data items in support of a specific operations function, such as provisioning.
Since global title information may be shared by several translation types, it is necessary for the STP to verify that the DPC and SSN that result from a GTT, to which the message will be routed, is valid (i.e., an equipped application resides at the end node).

**R4-264** [273] The STP shall verify the ability of the DPC and SSN to properly address the message through the use of the SCCP Application data described in Appendix J.

The following conditional requirements address the need to consolidate global title address ranges, to save memory space whenever possible.

**CR4-265** [274] Provided it does not place an undue processing burden on the STP, the STP shall consolidate and store GTT data with identical attribute values in the form of ranges whenever possible (e.g., for a given TT, the STP should consolidate ranges of GTAs in the existing GTT data model having identical DPC, SSN, relative cost, and routing indicator attribute values; similar range consolidation should be performed for GTT data stored via the multi-step GTT data model).

**CR4-266** [275] If the STP supports the above conditional requirement, it shall provide a mechanism to form, split, and reorganize such data ranges as data is added, deleted, and modified by SEAS recent change commands.

To eliminate or reduce the large number of event notifications generated due to customer dialing to vacant GTA codes, the STP is required to support the provisioning of a special argument “V” for the GTA attributes (e.g., DPC, SSN, and RI) that may be associated with GTT data. When the STP encounters a GTA code's attributes provisioned with the special argument “V” for a given GTA when performing a GTT for SS7 messages, the STP shall treat the event as a GTT failure of type “no translation for this address” as if no matching GTA entry was found and shall invoke UDTS/XUDTS message return procedures, if requested. However, the STP shall **not** generate failed-GTT event notifications (e.g., the REPT-NOTRNS message defined in Section 6.6.2) nor include the event in measurement peg counts of GTT errors. However, as a per-Bcc option, the STP may log events of this type in supplier-specific logging mechanisms to indicate to CCS network operations personnel that events of this type have occurred.

**R4-267** [276] The STP shall support the provisioning of the special argument “V” for GTA attributes defined by GTT data in Section 5 and Appendix J.

**R4-268** [277] The STP shall not generate failed-GTT event notifications nor include the event in GTT error measurements if the STP encounters a GTA with attributes provisioned with the special argument “V” when performing a GTT for a given SS7 message.
CR4-269 [278] As a per-Bcc option, the STP shall log the event associated with the STP encountering a GTA with attributes provisioned with the special argument “V” when performing a GTT for a given SS7 message.

Section 5.2.3 provides the data descriptions for GTT and SCCP application data that is required for STPs. Appendix J provides the related operations requirements and user’s views to support STP GTT data and SCCP application data. Refer to Section 4.3.3 for a description of the revised SCCP management procedures.

4.3.1.3 SCCP Hop Counter

The SCCP Hop Counter is a mandatory, fixed length parameter in the XUDT and XUDTS messages (see T1.112.3 of GR-246-CORE). Its purpose is to allow STPs to identify and discard messages involved in circular SCCP routing. STP processing of the SCCP Hop Counter parameter is considered in GR-246-CORE only in the context of GTT, but not ISNI routing. Hence, requirements for SCCP Hop Counter are addressed here as they apply both to GTT and ISNI routing.

The SCCP Hop Counter is initialized by the node originating the message. It is decremented by one each time an XUDT/XUDTS message is received by the SCCP from the MTP at an STP, except that the counter is not decremented if the STP receiving an XUDT/XUDTS message is also its final destination (i.e., from an application perspective). If the SCCP Hop Counter for an XUDT message is decremented to zero at an STP and the message specifies return on error, the STP will send an XUDTS message; otherwise, the received message is discarded. If the Hop Counter for a XUDTS message is decremented to zero, the STP shall discard that message. These STPs actions are stated in Requirements R4-270 [279], R4-271 [280], and R4-272 [281].

R4-270 [279] If an STP receives an XUDT or XUDTS message that requires SCCP routing and the STP is not the final destination for the received message (i.e., if the received routing indicator, which is the 7th bit in the address indicator octet in the SCCP Called Party Address is 0, meaning that further GTT is required), the STP shall decrement the SCCP Hop Counter by one.

R4-271 [280] If decrementing the SCCP Hop Counter results in a value of zero for an XUDTS message, the STP shall discard that message.

R4-272 [281] If decrementing the SCCP Hop Counter results in a value of zero for an XUDT message and that message specifies return on error, the STP shall send an XUDTS message to the Calling Party Address with a return cause indicating “SCCP Hop Counter violation.” Otherwise, the received XUDT message shall be discarded. If an XUDTS message is sent, the SCCP Hop Counter in that message shall be set to 15.
4.3.1.4 Return Cause Parameter in UDTS and XUDTS Messages

For a number of reasons (e.g., failure to perform a GTT, network congestion, link set outage), an STP may fail to transfer a UDT or XUDT message for which it has to perform a GTT. GR-246-CORE does not state how such failure should be mapped to a particular return cause in a UDTS or XUDTS message (a UDTS or XUDTS message is returned if message return on error is indicated in the received message). Such mapping is specified in Requirement R4-273 [282]. It should be noted that some of the terminology used in Requirement R4-273 [282] has changed in this issue, due to the expanded GTT capability in the ANSI T1 standard. Refer to Section 4.3.3.1 for definitions of the new terms.

R4-273 [282] When an STP fails to transfer a UDT or XUDT message for which it has to perform SCCP routing, the STP shall specify a return cause indicated below if it sends a UDTS or XUDTS message to the Calling Party Address in the received message:

- If the STP is unable to perform a translation because the global title indicator (a subfield of the address indicator parameter) in the received message is other than 0010, the return cause shall indicate “no translation for an address of such nature.”

- If the STP is not equipped with a GTT table corresponding to the translation type indicated in the Called Party Address of the received message, the return cause shall indicate “no translation for an address of such nature.”

- If the STP is equipped with the appropriate table, but cannot provide a translation for the particular global title address specified in the message, the return cause shall indicate “no translation for this specific address.”

- If the STP is unable to transfer the received message because of congestion on the route set towards the preferred destination (and does not attempt to send it to the next preferred destination - see Section 4.3.3.1), the return cause shall indicate “network congestion.”

- If the STP is unable to transfer the received message because of congestion on the route set towards the preferred destination and it attempts but fails to send the message to the next preferred destination (see Section 4.3.3.1), the return cause shall indicate “network congestion.”

- If the message destination signaling point is inaccessible (when translation results in only one destination), the return cause shall indicate “network failure.”
• If the destination signaling point is accessible but the destination subsystem is marked prohibited (when translation results in only one subsystem), the return cause shall indicate “subsystem failure.”

• If the message cannot be routed due to either an inaccessible destination or a prohibited subsystem, the return cause shall indicate the reason for failure with respect to the highest relative cost destination/subsystem (when translation may result in more than one destination). For example, if the translation may result in one of 4 destinations/subsystems, with relative costs 10, 20, 30 and 40, the return cause shall indicate the reason why the message could not be routed to the destination/subsystem with relative cost 40. If that destination signaling point was inaccessible, the return cause shall indicate “network failure.” If that destination signaling point was accessible, but the subsystem is prohibited, the return cause shall indicate “subsystem failure.”

• If the STP performing the final GTT (see Section 4.3.1.1) determines that the derived subsystem number is not equipped at the destination signaling point, the return cause shall indicate “unequipped user.”

• If the STP has decremented the SCCP Hop Counter for an XUDT message to a value of zero, the return cause shall indicate “SCCP Hop Counter violation.”

• If the STP receives an XUDT(S) (i.e., the STP recognizes the XUDT[S] message type) containing the optional SCCP ISNI parameter and can not perform the ISNI procedures, the return cause shall be “message incompatibility.”

• For other architecture-specific reasons for which the above return causes do not apply, the return cause shall indicate “unqualified.”

GR-246-CORE also does not state how an STP failure to transfer a UDT or XUDT message to a particular subsystem at the STP should be mapped to a particular return cause in a UDTS or XUDTS message. Such mapping is specified in Requirement R4-274 [283]. (Although OMAP currently sends UDT messages, the requirement below covers XUDT messages also in case they will be used in the future.)

R4-274 [283] When an STP fails to transfer a UDT or XUDT message to a particular subsystem at the STP, the STP shall use a return cause indicated below if it sends a UDTS or XUDTS message to the Calling Party Address in the received message:

• If the subsystem specified in the Called Party Address is unavailable due to a processing failure at the STP, the return cause shall indicate “subsystem failure.”
… • If the subsystem specified in the Called Party Address does not exist at the STP, the return cause shall indicate “unequipped user.”

… • For other, architecture-specific reasons for which the above return causes do not apply, the return cause shall indicate “unqualified.”

The return cause of “Subsystem congestion” is for further study.

The ISNI-specific return causes, to be specified in an XUDTS message when an STP is unable to transfer a message containing an SCCP ISNI parameter, are discussed in Appendix E. Also, refer to Section 4.3.1.4 for an additional return cause.

### 4.3.1.5 Verification of XUDT Message Processing Capability

In the future, end nodes may need to send messages using the new SCCP XUDT message type for reasons other than the ISNI capability. Initially, not all end nodes will recognize the new XUDT message type, and any nodes that do not will discard the message. To avoid this message loss, the STP will verify that the end node is capable of processing an XUDT message through the use of the SCCP Application data, described in Appendix J. An attribute in this entity will identify the point code and subsystem’s ability to process an XUDT message. Note that, if the SCCP in the end node is incapable of processing an XUDT message, all of the subsystems in the end node will also be incapable.

**R4-275** [284] If the STP performs the final GTT for an XUDT message that results in a destination point code and subsystem, the STP shall verify the ability of the point code and subsystem to properly process an XUDT message through the use of the Destination Data described in Section 5.

**R4-276** [285] If the STP determines that the point code and subsystem cannot properly process an XUDT message, the message shall fail. The STP shall perform message return procedures described in T1.112.4 of GR-246-CORE. If the message return procedures result in an XUDTS message being sent back to the originator of the XUDT message, the return cause shall be “unauthorized message.”

### 4.3.2 SCCP Connectionless Control

SCCP connectionless control denotes a set of procedures that allow a user of the SCCP to transfer up to 3904 octets of user data without establishing a signaling connection. Presently, the only SCCP user at an STP is OMAP.

**R4-277** [286] An STP shall provide SCCP connectionless control functionality as discussed in Section 4 of T1.112.4 of GR-246-CORE.
4.3.3  SCCP Management

SCCP management provides procedures to reroute or throttle traffic upon congestion in the network or failure of either the SCCP user or the signaling route to the SCCP user. It also provides procedures to share information on subsystem routing statuses between STPs performing the final GTT and SCPs with replicated subsystems. SCCP procedures complement MTP procedures for the signaling route management and flow control.

The ANSI T1 standard allows SCCP load sharing of traffic to an unlimited number of replicated node/subsystems. Although the ANSI T1 standard supports SCCP load sharing to an unlimited number of replicates based on equal cost, a Bcc network will require that an STP supports SCCP load sharing to up to 8 destinations assigned equal relative cost (see Section 4.3.1.1.3 for the requirements).

SCCP management procedures are impacted by the changes to the ANSI T1 standard, which are reflected in the most recent issue of GR-246-CORE. Since the changes to the SCCP management procedures appear in GR-246-CORE for the first time, they are also described in detail in Section 4.3.3.1 of this document.

R4-278  [287] An STP shall initiate and perform the SCCP management procedures listed below as described in Section 5 of T1.112.4 of GR-246-CORE, and also described in Section 4.3.3.1 of this document:

...  • For Signaling Point (SP) Status Management (see GR-246-CORE text in Section 4.3.3.1.1):

...  — SP Prohibited (Section 5.2.2 of T1.112.4 of GR-246-CORE)

...  — SP Allowed (Section 5.2.3 of T1.112.4 of GR-246-CORE)

...  — SP Congested (Section 5.2.4 of T1.112.4 of GR-246-CORE) - see additional requirements in Section 4.3.3.2.1 below.

...  • For Subsystem Status Management (see GR-246-CORE text in Section 4.3.3.1.2):

...  — Subsystem Prohibited (Section 5.3.2 of T1.112.4 of GR-246-CORE)

...  — Subsystem Allowed (Section 5.3.3 of T1.112.4 of GR-246-CORE)

...  — Subsystem Status Test (Section 5.3.4 of T1.112.4 of GR-246-CORE):

...  — Broadcast of Subsystem Prohibited (SSP) and Subsystem Allowed (SSA) Messages (Section 5.3.7 of T1.112.4 of GR-246-CORE) - see also additional requirements in Section 4.3.3.3 below.

...  • Traffic Information Management
… Traffic Information management procedures apply only to a replicated subsystem with a single backup (primary/secondary node/subsystem configuration)

… An STP in a Bcc network that performs final GTT shall perform the Traffic Information Management functions appropriate to the STP as discussed in Section 5.2, 5.3, and 5.4 of T1.112.4 of GR-246-CORE (note that they are considered optional in GR-246-CORE), for a replicated subsystem with a single backup operating in a dominant mode. Specifically, an STP shall be able to

… — Send Subsystem-Backup-Routing messages

… — Send Subsystem-Normal-Routing messages

… — Respond to Subsystem-Routing-Status-Test messages.

Note: these messages do not apply to nodes/subsystems operating in the loadshare mode. Therefore the following requirement applies:

R4-279 [288] The STP shall not send Subsystem-Backup-Routing or Subsystem-Normal-Routing messages upon changes in the status of loadshare node(s)/subsystem(s).

R4-280 [563] The STP shall only send Subsystem-Backup-Routing or Subsystem-Normal-Routing messages when there are two replicates operating in the dominant mode.

Since an STP presently does not have a subsystem duplicated at another SP, it does not have to perform the Coordinated State Change procedure described in Section 5.3.5 of T1.112.4 of GR-246-CORE.

Since the only SCCP user at an STP is presently OMAP, and since there are presently no requirements for the OMAP subsystem to keep track of the status of OMAP subsystems at other SPs, an STP in a Bcc network does not have to perform the Local Broadcast of subsystem status information described in Section 5.3.6 of T1.112.4 of GR-246-CORE. An STP also does not have to take any actions associated with a local broadcast for the SCCP management procedures that it is required to perform.

4.3.3.1 SCCP Management Procedures - Changes to GR-246-CORE

This section describes STP requirements for the SCCP management procedures listed above. Since some of the procedures are affected by the recent changes to the ANSI T1 standard to allow SCCP load sharing of traffic, and are described in GR-246-CORE for the first time, they are also described in this document. The changes to GR-246-CORE appear
in italics. Future issues of this document will reference GR-246-CORE with respect to SCCP management procedures, and the majority of this section will be removed from this document.

4.3.3.1.1  *SP Status Management* - *(Section 5.2 of T1.112.4 of GR-246-CORE)*

**SP Prohibited Control** - *(Section 5.2.2 of T1.112.4 of GR-246-CORE)*

When SCCP management receives an MTP-PAUSE indication relating to a destination that becomes inaccessible, SCCP management does the following:

1. Marks as “prohibited” the status of that signaling point
2. Initiates a local broadcast (Section 5.3.6) of “signaling point inaccessible” information for that signaling point
3. If the indicated signaling point is a preferred node, marks the translation as: “translate to the next preferred node” if that signaling point has a backup;
   
   *or,*
   
   *If the indicated signaling point is a loadshare node, marks the translation as “translate to the remaining available loadshare nodes.”* Otherwise, marks the affected node inaccessible
4. Marks as “prohibited” the status of each subsystem at that signaling point;
5. Discontinues any subsystem status tests (Section 5.3.4) it may be conducting to any subsystems at that signaling point
6. If the signaling point is a preferred node, marks the translation as “translate to the next preferred subsystem” for each subsystem at that signaling point for which a backup subsystem exists;
   
   *or,*
   
   *If the signaling point is a loadshare node, marks the translation as “translate to the remaining available loadshare subsystems” for each subsystem at that signaling point for which a loadshare subsystem exists.* Otherwise, marks the affected subsystems inaccessible
7. Initiates a local broadcast (Section 5.3.6) of “User-out-of-service” information for each subsystem at that signaling point
8. If the MTP-PAUSE pertains to the preferred node, and traffic will be diverted to the next preferred node, sends a Subsystem-Backup-Routing (SBR) message regarding

---

5. An SBR message is not sent for loadshare subsystems.
each replicated subsystem at that signaling point to SCCP management at the location of the corresponding next preferred subsystem. (This action is taken only if the node receiving the MTP-PAUSE is a “translator node” that is adjacent to the node at which the next preferred subsystem is located. For example, an STP which learns that an adjacent database has failed sends an SBR message to SCCP management for each replicated subsystem at the next preferred signaling point. If the STP is not adjacent to the next preferred subsystem, it does not send SBR messages.)

9. Marks all local equipped duplicated subsystems backup routed from the failed signaling point, if the failed signaling point is an adjacent translator node.

10. Initiates the traffic-mix information procedure (Section 5.4.2.1.1 of T1.112.4 of GR-246-CORE) to the local allowed users if the failed signaling point is an adjacent translator node.

11. Stops all subsystem routing status tests for the failed signaling point (Section 5.4.4 of T1.112.4 of GR-246-CORE).

**SP Allowed - (Section 5.2.3 of T1.112.4 of GR-246-CORE)**

When SCCP management receives an MTP-RESUME indication relating to a destination that becomes accessible, SCCP management does the following:

1. Marks as “allowed” the status of that signaling point
2. Resets the congestion level of that signaling point
3. Initiates a local broadcast (Section 5.3.6 of GR-246-CORE) of “signaling point accessible” information for that signaling (Note: this is not required for a Bcc STP.)
4. Marks the translations as: “translate to the previously inaccessible higher priority node,” if the signaling point is a replicated higher priority node,
   or
   Marks the translation as: “translate to all available loadshare nodes,” if the signaling point is a loadshare node
5. Except for selected replicated subsystems:
   — Marks as “allowed” the status of each remote subsystem;
   — Initiates a local broadcast (Section 5.3.6 of T1.112.4 GR-246-CORE) of “User-in-service” information for each subsystem at that signaling point;
   — Marks the translation as “translate to the previously inaccessible higher priority subsystem” for each replicated subsystem at the signaling point, if the signaling point contains replicated higher priority subsystems;

---

6. The Traffic Information Management Procedures are optional in GR-246-CORE signaling.
7. This refers to logical adjacency.
or

Marks the translation as “translate to all available loadshare subsystems” for each loadshare subsystem at that signaling point.

6. As a network provider option, the subsystem status can be marked as “prohibited”, for selected replicated subsystems (operating in either dominant or loadshare mode). For such subsystems, the subsystem status test procedure is initiated.

7. Initiates, if the recovered signaling point is an adjacent translator node, the following:
   a. The subsystem routing status test procedure (Section 5.4.4 of T1.112.4 of GR-246-CORE) for all local equipped replicated subsystems.
   b. The traffic-mix information procedure (Section 5.4.2.1.1 of T1.112.4 of GR-246-CORE) to the local allowed subsystems.

**SP Congested - (Section 5.2.4 of T1.112.4 of GR-246-CORE)**

When SCCP management receives an MTP-STATUS indication relating to signaling network congestion to a signaling point, SCCP management does the following:

1. Updates that signaling point status to reflect the congestion.
2. Initiates a local broadcast (Section 5.3.6) of “signaling point congested” information for that signaling point. (Note: this is not required for a Bcc STP.)

The congestion status of a signaling point may be used during translation to determine whether to route a received Class 0 message to the preferred signaling point/subsystem or to the next preferred signaling point/subsystem if the option is selected to alternate route messages because of signaling point congestion for the dominant mode (defined on a per-subsystem number basis for replicated subsystems operating in the dominant mode). If the loadshare mode is in use, the congestion status of a signaling point may be used during translation to determine if any of the loadshare nodes should NOT receive a Class 0 message due to congestion.

Note: For Bcc networks, if the option is selected, traffic for that subsystem with a priority less than the congestion level of the preferred signaling point will be alternate routed to the next preferred signaling point/subsystem, if the next preferred signaling point and subsystem are available and the next preferred signaling point has a congestion level less than or equal to the priority of the received message. For the loadshare mode, if this option is selected the congestion status of a loadshare node is used to determine if it should not receive a class 0 message.

This option should only be used for replicated applications (i.e., database services) that involve one message priority (e.g., all messages use priority 0) and use global title routing for the initial message.
4.3.3.1.2 Subsystem Status Management (Section 5.3 of T1.112.4 of GR-246-CORE)

Subsystem Prohibited

A. Receipt of Message for a Prohibited Subsystem:

If SCCP routing control receives a message, whether originated locally or not, for a prohibited local subsystem, SCCP routing control invokes subsystem prohibited control\(^8\). A Subsystem-Prohibited message is sent to the originating signaling point if the originating subsystem is not local (the OPC is a parameter in the MTP-TRANSFER indication primitive). The action, if any, to be taken, if the originating subsystem is local, is for further study.

B. Receipt of Subsystem-Prohibited Message or N-STATE Request Primitive or Local User Failed:

Under one of the following conditions:

1. SCCP management receives a Subsystem-Prohibited message about a subsystem marked allowed
2. An N-STATE request primitive with “User-out-of-service” information is invoked by a subsystem marked allowed
3. SCCP management detects that a local subsystem has failed, then SCCP management does the following:

   a. If the Subsystem-Prohibited message pertains to the preferred subsystem, marks the translation as appropriate: “translate to next preferred subsystem” if the prohibited subsystem is replicated.

   or

   If the Subsystem-Prohibited message pertains to a loadshare subsystem, marks the translation as appropriate: “translate to remaining available loadshare subsystems.”

   b. Marks as “prohibited” the status of that subsystem.

   c. Initiates a local broadcast (Section 5.3.6 of T1.112.4 of GR-246-CORE) of “User-out-of-service” information for the prohibited subsystem. (Note: this is not required for a Bcc STP).

   d. Initiates the subsystem status test procedure (Section 5.3.4 of T1.112.4 of GR-246-CORE) if the prohibited subsystem is not local.

---

8. SCCP Routing Control also invokes SCCP Connectionless Control for return treatment (see section 4.2 of T1.112.4) of the received message.
e. Forwards the information throughout the network by initiating a broadcast (Section 5.3.7 of T1.112.4 of GR-246-CORE) of Subsystem-Prohibited messages to concerned signaling points. The list of concerned signaling points should include, at a minimum, the mate subsystem. The list of concerned signaling points may also include replicates other than the mate subsystem, as well as other translator nodes with an immediate need to be informed of a particular change in status. The mate subsystem should be included in this list so that mates are aware of each other’s status for coordinated state change purposes. The concerned signaling points for a particular subsystem are determined by the network provider.

f. If the Subsystem-Prohibited message pertains to the preferred subsystem\(^9\), sends a Subsystem-Backup-Routing\(^10\) message to SCCP management at the location of the corresponding next preferred subsystem, if it has the translation capability and if the next preferred subsystem is located at an adjacent signaling point\(^6\).

g. Cancels “ignore subsystem status test” and the associated timer if they are in progress and if the newly prohibited subsystem resides at the local node.

h. Cancels “wait for grant” and the associated timer (coord.chg) if they are in progress and if the newly prohibited subsystem resides at the local node.

**Subsystem Allowed**

Under one of the following conditions:

1. SCCP management receives a Subsystem-Allowed message about a subsystem marked prohibited

2. An N-STATE request primitive with “User-in-Service” information is invoked by a subsystem marked prohibited,

then SCCP management does the following:

   a. If the Subsystem-Allowed message pertains to a higher priority subsystem, marks the translation as appropriate: “translate to previously inaccessible higher priority subsystem” if the subsystem is replicated;

      or,

      If the Subsystem-Allowed message pertains to a loadshare subsystem, marks the translation as appropriate: “translate to all available loadshare subsystems.”

   b. Marks as “allowed” the status of that subsystem.

---

9. The Traffic Information Management Procedures are optional in GR-246-CORE.

10. SBR message not sent for loadshare subsystems.
c. Initiates a local broadcast (Section 5.3.6 of T1.112.4 of GR-246-CORE) of “User-in-service” information for the allowed subsystem. (Note: this is not required for Bcc STPs).

d. Discontinues the subsystem status test relating to that subsystem if such a test was in progress.

e. Forwards the information throughout the network by initiating a broadcast (Section 5.3.7 of T1.112.4 of GR-246-CORE) of Subsystem-Allowed messages to concerned signaling points. The list of concerned signaling points should include, at a minimum, the mate subsystem. The list of concerned signaling points may also include replicates other than the mate subsystem, as well as other translator nodes with an immediate need to be informed of a particular change in status. The mate subsystem should be included in this list so that mates are aware of each other's status for coordinated state change purposes. The concerned signaling points for a particular subsystem are determined by the network provider.

f. If the Subsystem-Allowed message pertains to a higher priority subsystem, sends, if it has the translation capability, a Subsystem-Normal-Routing message to SCCP management at the node containing the previously preferred subsystem (i.e., the node that previously received the Subsystem-Backup-Routing message) if the previously preferred subsystem is located at an adjacent node.

g. Initiates the traffic mix information procedure (Section 5.4.2.1.1 of T1.112.4 of GR-246-CORE) if the newly allowed subsystem resides at the local signaling point.

**Subsystem Status Test**

No changes were made to the ANSI T1 standard, or GR-246-CORE, with respect to the subsystem status test procedure, as a result of the extension for SCCP load sharing capability.

**Broadcast of Subsystem-Prohibited (SSP) and Subsystem-Allowed (SSA) messages**

The broadcast of SSP and SSA messages is covered in the Subsystem Prohibited and Subsystem Allowed sections, respectively.

4.3.3.2 Additional Requirements for SCCP Management

The subsections below consider additional requirements for the SCCP management procedures in the following areas:

- SP Congested Control

---

11. The Traffic Information Management Procedures are optional.

12. An SNR message is not sent for loadshare subsystems.
• Broadcast of SSP or SSA Messages
• Performance Requirements.

4.3.3.2.1 Additional Requirements for SP Congested Control

If an STP can translate a global title into more than one subsystem for protocol class 0 messages, it may be advantageous to have the STP redirect traffic to the next preferred subsystem when congestion is encountered towards the point code corresponding to the preferred subsystem (for subsystems that the STP is routing traffic based on the dominant mode). If the STP is loadsharing traffic to a group of loadshare subsystems/point codes, it may also be advantageous to use the congestion status of a loadshare destination point code to decide if it should not receive traffic. An STP should provide a provisionable option to reroute traffic under such circumstances. This option is not addressed in detail in GR-246-CORE and hence is considered in Requirement R4-281 [289].

R4-281 [289] An STP shall provide an option, provisionable on a per-replicated-subsystem/DPC basis, that will specify “rerouting” or “no rerouting” when GTT for a protocol class 0 message results in a point code for a subsystem and the congestion status for that point code is higher than the priority of the message. No rerouting shall be the default. STP actions corresponding to the “no rerouting” option shall be as indicated in GR-246-CORE for the case of congestion (i.e., if message return on error is specified, a UDTS or XUDTS message is sent to the signaling point identified in the SCCP Calling Party Address of the received message with the return cause indicating “network congestion”; otherwise, the message is discarded; note that a transfer-controlled message is not returned by the STP in this case).

R4-282 [290] If the option specifies “rerouting” and the STP is routing to the subsystem/DPC base on the dominant mode, the message shall be rerouted to the next preferred subsystem if the following condition is met:

... The next preferred point code has a congestion status less than or equal to the priority of the message.

R4-283 [291] If the message is not rerouted to the next preferred subsystem because the condition is not met, the message shall be treated as if rerouting was not specified.

R4-284 [561] If the option specifies “rerouting” and the STP is loadsharing traffic to that subsystem/DPC, the message shall be rerouted to one of the other loadshare subsystems/point codes in the group which has a congestion status less than or equal to the priority of the message.
NOTE: The mechanism for SCCP loadsharing is vendor specific. Therefore, the decision process to decide which of the remaining loadshare subsystem/point codes from the group should receive the message when a particular loadshare signaling point is congested is also vendor specific.

**R4-285** [562] If the message is not rerouted to another loadshare subsystem/point code in the group because the condition in **R4-284** [561] is not met, the message shall be treated as if rerouting was not specified.

Section 5.2.3 provides the data description and Appendix J provides the related operations requirements and user’s views to support the option to alternate route traffic on congestion.

### 4.3.3.2.2 Additional Requirements for the Broadcast of Subsystem Prohibited or Allowed Messages

GR-246-CORE does not state explicitly that the list of concerned SPs, to which an SSP or SSA message should be broadcast according to the rules in Sections 5.3.7.2 and 5.3.7.3 of T1.112.4 of GR-246-CORE, should be provisionable. This is addressed in Requirement **R4-286** [292].

**R4-286** [292] The list of concerned SPs at an STP shall be provisionable on a per-subsystem (for a given node) basis. The STP shall broadcast an SSP or SSA message to each of the point codes on the list according to the rules in Sections 5.3.7.2 and 5.3.7.3 of GR-246-CORE.

Since it is likely that concerned SP lists will be the same for several applications, it may be more efficient to allow multiple applications to reference the same list of concerned SP lists.

**CR4-287** [293] As a per-Bcc option, the STP shall permit the provisioning of a reusable list of concerned signaling points that can be shared by more than one application.

Appendix J provides the related operations requirements and user’s views to support the sharing of concerned SP lists.

### 4.3.3.2.3 Additional Performance Requirements

The following performance requirement shall apply to an STP:

**R4-288** [294] An STP shall change the status of a subsystem to prohibited or allowed within 0.4 seconds of the trigger event that caused the change.

A trigger event may be:
• Receipt of an SSP or SSA message
• Link set outage that results in a destination becoming inaccessible
• Link set restoration that results in a destination becoming accessible
• Receipt of a TFP/TCP message
• Receipt of a TFA/TCA message.

**R4-289**  
[295] An STP shall be able to commence broadcast of SSP or SSA message to the appropriate SPs within 0.4 seconds of the receipt of an SSP or SSA message for the prohibited or allowed subsystem.

### 4.3.4 Processing of SCCP Network Management Tasks During Processor Overload

This subsection considers STP processing of SCCP network management tasks during processor overload, a topic not addressed in GR-246-CORE.

**R4-290**  
[296] The SCCP management function shall be designed in such a way that during the overload of the STP network management processor(s), processing of critical SCCP management tasks will be given high priority. A possible description of this capability is described in Section 4.2.4.18 of this document and in Appendix G.

SCCP management tasks refer to functions provided by the STP processor(s) responsible for SCCP management functions described in Section T1.112.4 of GR-246-CORE.

The following additional requirements are considered applicable to support this capability in STPs.

**O4-291**  
[297] The STP SCCP management tasks shall be assigned a priority within a priority range of 0 to 3, with 3 being the highest priority and 0 being the lowest priority.

**R4-292**  
[298] The STP shall assure that prioritized processing of SCCP management tasks does not result in incorrect subsystem status information. For example, if a SSP is received followed by a SSA for a subsystem, the final status of the subsystem should be considered allowed.

**R4-293**  
[299] In addition, the STP shall comply with other requirements described in Section 4.2.4.18.

**O4-294**  
[300] Specific assignments of priorities to SCCP management tasks should be based on the SCCP management principles used in the STP.
Appendix G provides guidelines for assigning priorities to SCCP management tasks.

4.4 Operations, Maintenance, and Administration Part (OMAP)

The STP shall support MTP Routing Verification Test (MRVT) and SCCP Routing Verification Test (SRVT) defined in OMAP. The requirements for these tests may be found in GR-1245-CORE and in T1.116 of GR-246-CORE. The MRVT and SRVT will detect incompleteness or errors in MTP routing and GTT tables, respectively.
Figure 4-1. Relationship Between Far-End PC of Link Sets at STPs and Primary PC of Multiple PC SPCS

From STP1 and STP2, far end point code for both A1 and A2 is X

At multiple point code SPCS, primary point code should be X

Figure 4-2. Adjacent STP View of a Multiple PC SPCS

Adjacent STP’s view of a multiple point code SPCS with point code X,Y,Z

multiple point code SPCS with point codes X,Y,Z
A and F are SEPs. B, C, D, and E are STPs. The normal (highest priority) route from STP E to A is the E-link set shown by the dashed line and marked by (1). The first alternate route is the C-link set to mated STP D marked by (2). The second alternate route is the combined B-link set to STPs B and C marked by (3). Note that this example assumes that cluster routing is not used for node A’s cluster. If an STP has a direct E-link set to a node and cluster routing is used for other members within that node’s cluster, requirement CR4-14 [559] specified the E-linkset must be the lowest priority route.
5. Operation Requirements

5.1 Overview of the Operational Environment

R5-1 [301] STPs must be operated through manual interactions (on-site and remote), and through mechanized system interfaces in the Bcc environment. The STPs must be operated remotely because many of them will be located in unattended COs. At times, however, Bcc technicians in the STP switch office will need on-site operational capabilities. This overview briefly describes the operations environments and functions for STPs.

Operations of STPs include functions grouped into provisioning, administration, maintenance, and network management. STP provisioning (described in Section 5.2) includes generic program alteration, loading and modifying recent changes, and backing up recent change tables. Administration (described in Section 5.3) involves collecting traffic and performance measures for equipment use studies, network usage accounting, and network planning. STP maintenance (described in Section 6) includes STP system maintenance, signaling link maintenance, and CCS network maintenance. Network management (described in Section 7) includes collecting near real-time surveillance data to detect network congestion and overseeing automatic controls in STPs to maximize network use.

R5-2 [302] The manual operations environment includes both on-site and remote operations. For on-site operations, the STP shall have a control and display interface for activating alarms, displaying system status and diagnostic error codes, and providing emergency reinitializations. Manual operations from a remote site should be the same as on-site operations.

R5-3 [303] The STP must be capable of providing direct communications to the remote site through either private line or a secure dial-up connection.

R5-4 [304] In the mechanized operations environment, the STP shall be capable of being supported by several OSs.

One such OS will be the SEAS system. The SEAS system will interface with STPs to support administration that will allow the user to collect and analyze measurements on traffic, equipment use, and performance. The SEAS system will also support provisioning functions that allow the user to generate and load assignments into STPs and provide backup for STP routing and assignment databases.

Operations support is also required for STP and signaling link maintenance. The SCCS will be used to support STP maintenance in the

Standardized interfaces are used for both the manual and the mechanized environments. The communications protocols are specified for person-to-system interfaces and system-to-system interfaces, which are discussed in Section 8.

### 5.2 STP Provisioning Requirements

The STP shall be capable of supporting the provisioning requirements described below.

Resource provisioning is directly related to engineering functions. It refers to the operations activities associated with making network facilities and equipment available for use. In addition to the construction and physical installation activities, resource provisioning includes installing software programs and data necessary to make the network element operational. Provisioning requirements for the STP include generic program alteration and Recent Change and Verification (RC&V) functions. Database management capabilities are also required to support the provisioning function in the STP.

#### 5.2.1 Generic Program Alteration

*R5-5 [305]* Requirements for generic program alteration are in TR-TSY-000541, *LSSGR: Measurements and Administration, Sections 8.2-8.6*.

*O5-6 [306]* In addition, it is highly desirable that generic updates and changes can be loaded into the STP via a communications link, under Bcc personnel control. This would require a secure link, possibly dial-up. Security requirements are considered in Section 8.

#### 5.2.2 STP Recent Change and Verify (RC&V) Functions

*R5-7 [307]* The STP shall provide RC&V functions as described below.

The RC&V functions refer to a collection of processes needed to administer the assigned values in the STP routing translation databases and provision signaling links. Commands are entered via the work position interfaces for an STP or via the STP-SEAS system interface. These functions should include the following:
• Recent Change: Update of the translation database
• Verify: Retrieval of sections of the translation database.

The role of the STP in the RC&V process is to
• Receive appropriate login requests from authorized users at an STP work position
• Provide an acceptance or rejection message in response to the login or session requests to the STP work position
• Accept valid or reject invalid RC&V messages
• Process the RC&V commands and return status information when necessary
• Return positive or negative acknowledgments as each command is processed or not processed
• Log RC commands on an external device
• Provide on-occurrence notification when errors in MTP routing are detected
• Provide on-occurrence notification when errors in SCCP routing are detected.

These procedures are detailed in the STP/SEAS system interface specification discussed in GR-310-CORE.

**R5-8** [308] The STP shall accept bulk loads (other than manual input) of RC commands to support database assembly and database restoration.

**R5-9** [309] It is desirable that the STP support bulk loading of recent changes via magnetic tape or other suitable program storage mechanisms.

**R5-10** [310] The STP shall provide a capability to enter RC&V commands from an on-site work position.

**O5-11** [311] In addition, it is desirable that the STP provide a capability to enter RC&V commands from a remote work position. This capability is intended to be used primarily during emergency situations. The STP shall implement a database lockout mechanism so that RC data cannot be corrupted because of simultaneous access from on-site and remote work positions.

**R5-12** [312] The STP shall also implement a database lockout mechanism so that RC data cannot be corrupted because of simultaneous access from the work positions and SEAS system interface.
5.2.3  STP Data Description

The following information contains the STP data model and related terminology associated with entity set/relationship models for databases. This is used for ease of expression and comprehension, and is meant to imply nothing about the expected or required structure of the STP database. The data model presented in this section is the blueprint of the STP data.

The next subsection gives an overview of the terminology for the information modeling used in this document. Following that, in sequence, are the STP data model diagrams, the STP data model’s entity, relationship and attribute dictionary, a discussion of the data operations or transactions, and the relationship of user views to the logical data model. Specific data format requirements relating to the SEAS system and RC&V messages are specified in Section 7.1 of GR-310-CORE.

5.2.3.1  Overview of Information Modeling Methodology

Traditionally, data (or information) has been described in an ambiguous, incomplete, and/or inconsistent manner, e.g., informal description, specific interface descriptions, etc. This leads to data consistency and data redundancy management problems across the entire enterprise, e.g., the same name for two data items but different meanings, different names for two data items but the same meaning, etc. The construction of an information model or Logical Data Model (LDM) is the process of defining “logical data structures” for use within an enterprise or portion of an enterprise (e.g., SS7) where that information model becomes the formal common understanding of data in the enterprise (or portion of an enterprise).

The information model provides a detailed representation of the logical data structures. The logical data structure representation shows entities (i.e., information entities: classes of abstract “things” in an enterprise, e.g., line or trunk) and relationships (i.e., information relationships: abstract associations between entities) in the information model. Furthermore, the information model may facilitate the design of databases to be used within an enterprise. A major benefit gained by the information model effort is the opportunity of viewing the data in a real world environment without considering any physical database system limitation or the efficiency of data storage, retrieval, and updating. In other words, an information model is the formalized description of the data (within an enterprise) with a common language that is independent of the target physical system. Since it is not constrained by any physical implementation concern, an information model of an enterprise can be understood, used, and appreciated by developers, systems engineers, planners, and end-users of enterprise systems.

The information model methodology used in this section is consistent with Bellcore’s information modeling guidelines described in SR-OPT-001826, Information Modeling Concepts and Guidelines. According to the methodology, the information that is kept about a logical model should be divided into the Extended Entity-Relationship (EER)
diagrams and the data dictionary. EER diagrams provide a graphical representation of a conceptual data schema without providing all of the details. The data dictionary is where the total set of information for an information model is kept.

The following subsections give an overview of the EER method (including the definition of symbols used in the EER diagrams) and the data dictionary. For a more detailed description of EER methodology and its relationship to Object-Oriented Methodology, see SR-OPT-001826.

**Extended Entity-Relationship Model**

Entity-Relationship (E-R) logical modeling method was originally proposed by P. P. Chen in 1976. The main items of this method are as follows: Entity, Relationship, and Attribute. Chen’s original E-R concepts have evolved throughout the years. This methodology has been extended with the addition of abstractions and generalization techniques into EER. The following subsections provide a brief discussion of the concepts of EER methods and diagrams.

**Entity**

An entity is a class of primary “things” (or objects) which can be easily distinguished from other classes of “things” (or objects) in an enterprise. Generally, entities are considered to be stand alone objects with distinct characteristics. However, the entity concept is not limited to a real world (i.e., physical) object. An entity can be an “abstract” object, as long as it is distinguishable from other entities. For instance, subscriber, service, and network element can be defined as entities in a TelCo’s enterprise. Although subscriber and network element represent physical objects, service can represent an abstract object.

An entity set is a collection of the same type of objects that are still distinguishable. It should be pointed out here that information modelers commonly use the term “entity” to mean “entity set.” This section follows this common practice. If an entity is called by its name (e.g., signaling point), it is understood to mean the set of things known as “signaling point” in the enterprise. To single out a specific member (known as an instance) of the set, the specific instance must be identified. For example, if a specific information model contains a set of signaling points called the SP entity and the information modeler’s interest is to identify a specific SP (e.g., switch A) represented by the SP entity, then the unique identifier (e.g., \( SP.ID = \) primary PC of switch A) must be specified along with the entity name (SP). In EER diagram notation, entities are represented by rectangles (Figure 5-1).

**Relationship**

A relationship is an association among entities. The relationships contained in an information model are limited to the relationships that are useful to the enterprise. For example, the relationship link termination may provide a very important association between link and port entities from the enterprise view of SS7 data. In EER diagram notation, relationships are represented by diamond shapes (see Figure 5-2).
Generally, relationships are defined between different entities. But, there is often a need for relationships between instances of the same entity set. The number of participating entities in a relationship determines the degree of the relationship.

Set and instance rules, discussed above for entities, also apply to relationships. A relationship is the set of “association instances” such that the necessary information from one instance of each of the participating entities is combined into a single instance of the relationship. An instance of the link termination relationship is the combination of an instance of link and an instance of port (i.e., a specific link and the port on which it terminates).

The relative participation of each entity in the relationship is known as the cardinality of these entities. The maximum cardinality of a participating entity in a relationship refers to the maximum number of permitted instances of that participating entity that can be associated with a given (single) instance of the other participating entity. The maximum cardinality of “one” for a participating entity in a relationship refers to the maximum of one permitted instance of that participating entity that can be associated with a given (single) instance of the other participating entity. The maximum cardinality of “many” for a participating entity in a relationship refers to many permitted instances of that participating entity that can be associated with a given (single) instance of the other participating entity. Instance(s) of Entity-A may participate with instance(s) of Entity-B in a given relationship based on one of the following maximum cardinalities:

- Many-to-many, N:M
- One-to-many, 1:N
- Many-to-one, N:1
- One-to-one, 1:1.

There are also minimum cardinalities for entity instances participating in a relationship. The terms mandatory and optional imply the type of minimum participation. If every instance of an entity must participate in the relationship, the entity’s participation in the relationship is called mandatory participation. Otherwise the entity’s participation is known as optional. The following symbols are used to convey the minimum/maximum cardinalities of entities [(Entity-A):(Entity-B)] in a relationship:

- $(X,Y):(P,Q)$

  - Where $X$ is the minimum participation of Entity-A and $P$ is the minimum participation of Entity-B in a given relationship. The possible values for $X$ and $P$ are 0 (optional participation) and 1 (mandatory participation).

- Where $Y$ is the maximum participation of Entity-A and $Q$ is the maximum participation of Entity-B in a given relationship. The possible values for $Y$ and $Q$ are N or M (to indicate many) or 1 (to indicate one).

The following are examples of minimum/maximum combinations:
• (1,N):(1,M) - Both entities have mandatory participation (minimum) and many-to-
many participation (maximum).
• (0,1):(1,N) - Entity-A has optional participation (minimum) and Entity-B has mandatory participation (minimum). There is a one-to-many (maximum) relationship here.

As a possible TelCo enterprise example, the participations of subscriber and service in the subscription relationship are mandatory (minimum), since every subscriber must have at least one service. This relationship would also be many-to-many (maximum) since a given instance of service can participate with many instances of subscriber and vice versa. In the example in Figure 5-2 (an STP data example), the participations of link and port in the relationship are optional (minimum). This relationship would also be one-to-one (maximum) since a given instance of link can participate with only one instance of port and a given instance of port cannot be associated with many instances of link via the link termination relationship (Figure 5-2).

Extensions to Basic E-R Monitoring
Abstraction and generalization techniques are the extensions to basic E-R modeling. The various kinds of abstractions and generalizations can subclassify, declare dependencies, etc. for the instances of an entity. The extensions defined here are: Associative Entity, Composite, Dependent, Member, Subtype, and Multi-Source Role.

Associative Entity
An associative entity is a relationship that also serves as an entity in its own right. There are situations where a particular object seems to meet the qualification criteria of both entity and relationship. This is encountered, for example, when the object contains relationship information and it needs to participate in other relationships. In Figure 5-3 the link set relationship between Adjacent SP and STP may be viewed as an entity that associates with Destination via the ordered route relationship. An associative entity is diagramed by a diamond in a rectangle frame (Figure 5-3).

Composite Entity
Some situations require a logical collection of different entities to create an entity superset called Composite (or aggregate). The entities that are part of the composite entity, which are called Component entities, do not inherit the attributes of the composite entity via this association, rather the component entities are “contained” in the composite entity. For example, the capability group entity can be viewed as a composite entity with STP. A composite entity is depicted as a line running from the composite entity into the apex of a triangle labeled with the letter C and with lines running out of the opposite side of the triangle to the component entities (Figure 5-4).

Dependent Entity
Some entities existence depends on the existence of another entity. For example, the relationship between the SSP and SSP application entities is “existence” dependent. In
other words, one cannot think of the existence of a specific SSP application without a specific SSP. Therefore, *SSP application* is a dependent entity on the *SSP* entity.

In information model diagrams, a dependency is depicted in the same way as a composite, except that the triangle is labeled with the letter **D** (Figure 5-5).

**Member Entity**

The Member Entity concept is used to demonstrate a special case that goes between the cases illustrated by the dependent and composite/component entity abstraction methods. The member entity is dependent on a superset entity that is the aggregate of the same kind of entities like itself (which is contrary to the composite entity case). Also, a member entity cannot exist without that superset entity. An example for dependent entity may be given from the STP Data Model in Section 5.1.8. The *Link entity* is the member of Link Set (a superset entity). A *Link* entity cannot exist if there is no *Link Set*. The components of *Link Set* are the same kind of entities (e.g., *Link*).

In information model diagrams, a member entity is depicted in the same way as a dependent entity, except that the triangle is labeled with the letter **M**.

**Subtype Entity**

Entities that constitute non-intersecting subsets of a larger entity set (superset) are called the **Subtype** to create a hierarchy of entity sets with an increasing level of detail as one proceeds *downward* in the hierarchy. For example, in the Figure 5-6, the entity *Destination* may be divided into several non-intersecting subentities (*Cluster, SP, and Capability Group*). In information model diagrams, a subtype is depicted as a line running from the superentity into the apex of a triangle labeled with the letter **S** and with lines running out of the opposite side of the triangle to the subentities (Figure 5-6).

Subtypes inherits all of the attributes (attribute is defined below) of their supertype. In addition, each subtype typically has unique attributes of its own. Although the relationships participated by the supertype are also inherited by its subtypes, each subtype may participate in its own relationships with other subtypes inside of its hierarchy as well as other entities outside of its hierarchy.

**Multi-Source Role**

Different entities that play the same role with respect to participation in a relationship can be modeled using the **Multi-Source Role**\(^1\) abstraction. In Figure 5-7, *remote SP*, and *adjacent SP* are the role sources (i.e., “actors”) for the *SP* multi-source role entity with respect to the *ordered route* relationship of *destination*, the superset of *SP* with *link set*. This abstraction provides for less complicated diagrams and a more concise data dictionary to convey the information.

---

1. The Multi-Source Role abstraction is currently not defined in Bellcore’s information model methodology (SR-OPT-001826). This role abstraction should not be confused with other “role” abstractions that may be defined in other environments.
A role is depicted in the same way as a subtype, dependent, etc. except that the triangle is labeled with the letter $R$ and points to the role sources (Figure 5-7).

**Attribute**

An attribute is a unit of information that describes a property of a particular entity or a particular relationship. Attributes provide facts (or properties) about entities and relationships. An entity instance or relationship instance is established when the attributes (of the particular entity or relationship) are assigned specific values.

The unique identifier (i.e., key attribute) of an entity or a relationship is the attribute that determines the specific instances of entities or relationships in the entity or relationship set. Thus, other attributes of entities or relationships are referred to as non-key attributes.

Attribute names defined for an entity or relationship should not be shared with any other entity or relationship. If similar non-key attributes are needed for other entities or relationships because of data requirements (controlled redundancy), aliases are created and clearly identified in the data dictionary.

For convenience, the unique identifier for a given relationship are chosen as the concatenation of the participating entities’ unique identifiers. However, associative entities (which are also relationships) usually have their own specific identifiers and, as other attributes, the identifiers of the entities that they associate. Relationships may also have some non-key attributes that do not belong to any other participating entities.

**Data Dictionary**

The data dictionary of an information model is the repository for all available information about that information model. There are primarily two sections in the data dictionary: **Entities and Relationships** and **Attributes**.

In the data dictionary all of the entities (including associative, subtype, role and aggregate entities) created in EER diagrams are defined according to a specific entity profile. An entity profile contains information about that specific entity, such as its name, alias, description, purpose, primary key, list of attributes, etc.

Similarly, the data dictionary contains information about each relationship and attribute that are created in an information model by populating the corresponding relationship and attribute profiles. A relationship profile holds information about a specific relationship, such as its name, aliases, description, purpose, primary key, list of attributes, related entities, degree, cardinality. An attribute profile holds information about a specific attribute, such as its name, aliases, description, purpose, affiliated entity or relationship, value domain, etc.

5.2.3.2 **STP Entity/Relationship Diagrams**

There are four Entity/Relationship diagrams provided for the STP data model in this document. The first diagram (Figure 5-8) depicts the MTP routing related entities and
relationships. The principal information conveyed by this diagram for MTP routing is that the *Link Set* associative entity participates in the *Ordered Route* relationship with the *Destination* entity. By using the EER abstraction and generalization techniques described in previous subsection, the Destination entity represents three different types of MTP destinations (i.e., *Cluster*, Signaling Point-SP, or *Capability Group*). Based on the CCS network architecture, SPs can be classified further as Signaling End Points-SEPs and STPs. Moreover, there are three different types of SEPs: Common Channel Signaling Switching Office-CCSSO, Service Switching Point-SSP, and Service Control Point-SCP. Also, the roles of SPs are presented here as the *Remote SP* and *Adjacent SP* entities. Adjacent 2SPs are the SPs that have the *Link Sets* terminating at the STP. For proper cluster routing, the Cluster must have remote SPs that have no Link Sets terminating at the STP. Another important aspect regarding the Link Sets shown in Figure 5-8 is the *Gateway Link Set* role that connects the STP with an SP in another CCS network (CCS network interconnection). As a member of a specific Link Set, the *Link* terminates at one specific *Port* of the STP. For proper cluster routing, the Cluster must have remote SPs that have no Link Sets terminating at the STP. Another important aspect regarding the Link Sets shown in Figure 5-8 is the *Gateway Link Set* role that connects the STP with an SP in another CCS network (CCS network interconnection).

The second diagram (Figure 5-9) depicts the SCCP routing related entities and relationships. The *Global Title* associative entity, that is also a relationship between the *Global Title Address* and *Translation Type* entities, participates in the *Ordered Global Title Translation* relationship to derive the *SCCP Destination*. The SCCP Destination may be a final destination at which the CCS service application is located (i.e., the *SCCP Application*) or a destination for an STP pair (i.e., *Capability Group*) where another Global Title Translation will be performed. Since not all Translation Types are standardized today, some Translation Types used by the foreign CCS networks have to be mapped to the Bcc specific Translation Types per Gateway Link Set basis. Therefore, *Existing Translation Type* entities are mapped to *Mapped Translation Type* entities by the *Translation Type Mapping* relationship on a Gateway Link Set basis depending on the direction of SS7 message traffic (i.e., incoming or outgoing). Also, based on specific SCCP Application (i.e., an *SCP Application* or an *SSP Application*), the STP needs to keep track of a provisioned SP list by the *Concerned Signaling Points* relationship to inform the application failure. The SCP applications may also have mates as indicated by the *SCP Application Mating* relationship.

The entities and relationships shown in Figure 5-10 and Figure 5-11 portray the Gateway Screening data model of the STP. Using the EER generalization and abstraction techniques, entities like *Allowed OPC*, *Allowed DPC*, *Blocked OPC*, etc. (as depicted in Figure 5-1) are introduced. These entities participate in *MTP NM Screening Criteria*, *MTP T&M Screening Criteria*, *ISDNUP Message Type Screening Criteria*, *TCAP Query Screening Criteria*, *TCAP Response Screening Criteria*, *Unitdata Service Screening Criteria*, and *SCCP 2.*

The terms “Adjacent” and “Remote” are used here to allude to the physical connectivity of some SPs with the STP via CCS links based on the CCS network configuration. If an SP is connected to the STP with a CCS link, it is considered to be adjacent to the STP. If there is no link between an SP with the STP, that SP is remote to the STP. For the time being, these definitions apply only to the STP Data Description section of this document. One should distinguish the context driven meanings of these terms in other CCS documents, which might be different than here.
Management Criteria relationships (Figure 5-11) to represent the provisioned gateway screening data in the STP.

Definition of these entities, relationships and attributes are given as data dictionaries in following subsections.

5.2.3.3 STP Entity Data Dictionary:

<table>
<thead>
<tr>
<th>Entity Name</th>
<th>Description</th>
<th>Entity Type</th>
<th>Key Attribute(s)</th>
<th>Other Attributes</th>
<th>Relationships</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjacent SP</td>
<td>Adjacent SP is an entity set that represents various types of CCS nodes which are interconnected with the STP via a Link Set.</td>
<td>Role of SP entity</td>
<td>clli</td>
<td>point_code</td>
<td>Ordered Route Link Set (Associative Entity)</td>
</tr>
<tr>
<td>Allowed Affected Destination</td>
<td>This entity set plays the role of specific SPs that receiving MTP network management messages about these SPs are allowed according to one (or more) existing MTP NM Screening Criteria.</td>
<td>Role of SP Entity</td>
<td>allowed_affected_destination</td>
<td>none</td>
<td>MTP NM Screening Criteria</td>
</tr>
<tr>
<td>Allowed Affected PC/SSN</td>
<td>This entity set plays the role of specific SCCP Applications that receiving SCCP management messages about these applications are allowed according to one (or more) existing SCCP Management Screening Criteria.</td>
<td>Role of SCCP Application entity</td>
<td>allowed_affected_pc_ssn</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>
Relationships:  SCCP Management Screening Criteria

Entity Name:  Allowed DPC (Destination Point Code)
Entity Type:  Role of SP Entity
Description:  This entity plays the role of specific SPs that the SS7 messages destined for those are allowed according to one (or more) existing gateway screening criteria.
Key Attribute(s):  allowed_dpc
Other Attributes:  none
Relationships:  MTP NM Screening Criteria
               MTP T&M Screening Criteria
               ISDNUP Message Type Screening Criteria
               TCAP Query Screening Criteria
               TCAP Response Screening Criteria
               Unitdata Service Screening Criteria
               SCCP Management Screening Criteria

Entity Name:  Allowed ISDNUP Message Type
Entity Type:  Entity
Description:  This entity provides information about allowable ISDNUP message types according to one (or more) existing gateway screening criteria.
Key Attribute(s):  allowed_isupmt
Other Attributes:  none
Relationships:  ISDNUP Message Type Screening Criteria

Entity Name:  Allowed OPC (Origination Point Code)
Entity Type:  Role of SP entity
Description:  This entity plays the role of specific SPs whose specific SS7 messages are allowed according to one (or more) existing gateway screening criteria.
Key Attribute(s):  allowed_opc
Other Attributes:  none
relationships:  MTP NM Screening Criteria
               MTP T&M Screening Criteria
               ISDNUP Message Type Screening Criteria
               TCAP Query Screening Criteria
               TCAP Response Screening Criteria
               Unitdata Service Screening Criteria
               SCCP Management Screening Criteria

entity name:  **Allowed CDPA (Called Party Address)**
entity type:  Role of SCCP Application entity
description:  This entity set plays the role of specific SCCP Applications that sending specific SS7 messages to these applications are allowed according to one (or more) existing gateway screening criteria.

key attribute(s):  allowed_cdpa
other attributes:  none
relationships:  TCAP Query Screening Criteria
                TCAP Response Screening Criteria
                Unitdata Service Screening Criteria
                SCCP Management Screening Criteria

entity name:  **Allowed CGPA (Calling Party Address)**
entity type:  Role of SCCP Application entity
description:  This entity set plays the role of specific SCCP Applications that receiving specific SS7 messages from these applications are allowed according to one (or more) existing gateway screening criteria.

key attribute(s):  allowed_cgpa
other attributes:  none
relationships:  TCAP Query Screening Criteria
                TCAP Response Screening Criteria
                Unitdata Service Screening Criteria
                SCCP Management Screening Criteria

entity name:  **Allowed Signaling Information Octet (SIO)**
entity type:  Regular Entity
Description: Allowed SIO entity provides information about allowable types and priorities of the received SS7 messages according to one (or more) existing gateway screening criteria.

Key Attribute(s): allowed_sio
Other Attributes: none
Relationships: MTP NM Screening Criteria  
MTP T&M Screening Criteria  
ISDNUP Message Type Screening Criteria  
TCAP Query Screening Criteria  
TCAP Response Screening Criteria  
Unitdata Service Screening Criteria  
SCCP Management Screening Criteria

Entity Name: Allowed Translation Type
Entity Type: Role of Translation Type entity
Description: This entity plays the role of specific Translation Types (indicated by the received SS7 messages) that are allowed according to one (or more) existing TCAP Response Screening Criteria.

Key Attribute(s): allowed_tt
Other Attributes: none
Relationships: TCAP Response Screening Criteria

Entity Name: Blocked DPC (Destination Point Code)
Entity Type: Role of SP entity
Description: This entity set plays the role of specific SPs that the SS7 messages destined to these SPs are blocked according to one (or more) existing gateway screening criteria.

Key Attribute(s): blocked_dpc
Other Attributes: none
Relationships: MTP NM Screening Criteria  
MTP T&M Screening Criteria  
ISDNUP Message Type Screening Criteria  
TCAP Query Screening Criteria  
TCAP Response Screening Criteria
Entity Name: **Blocked OPC (Origination Point Code)**

**Entity Type:** Role of SP entity

**Description:** This entity plays the role of specific SPs whose specific SS7 messages are blocked according to one (or more) existing gateway screening criteria.

**Key Attribute(s):** blocked_opc

**Other Attributes:** none

**Relationships:**
- MTP NM Screening Criteria
- MTP T&M Screening Criteria
- ISDNUP Message Type Screening Criteria
- TCAP Query Screening Criteria
- TCAP Response Screening Criteria
- Unitdata Service Screening Criteria
- SCCP Management Screening Criteria

Entity Name: **CCSSO (CCS Switching Office)**

**Entity Type:** Subtype of SEP entity

**Description:** CCSSO entity set represents all switching offices that are equipped with the CCS technology but do not provide the SSP capabilities.

**Key Attribute(s):** clli

**Other Attributes:**
- primary_point_code
- number_of_point_codes
- point_code_list

**Relationships:** Ordered Route

Entity Name: **Capability Group**

**Entity Type:** Subtype of Destination entity

**Description:** Capability Group entity set identifies a logical group of functionally related STPs to relay SS7 messages to their final destination. This is useful in MTP routing process to route SS7 messages to remote STPs (which are mated STPs) without concerning their individual network status (e.g., congested, unavailable, etc.).
**Key Attribute(s):** capability_code

**Other Attributes:** (This entity may have additional attributes like “capability_group_list” to identify other components (STPs) in a given capability group.)

**Relationships:** Ordered Route

**Entity Name:** Cluster

**Entity Type:** Subtype of Destination entity

**Description**  
Cluster entity set is a specific collection of the Remote SPs that the STP may use the cluster routing process to send SS7 messages to those Remote SPs.

**Key Attribute(s):** cluster_code

**Other Attributes:**  
- network_cluster_exception_list_exclusion_indicator
- network_cluster_broadcast_exception_list
  (This entity may have additional attributes like “sep_point_code_list” to identify other components (Remote SPs) in a given cluster.)

**Relationships:** Ordered Route

**Entity Name:** Destination

**Entity Type:** Superset Entity

**Description**  
The Destination entity set provides the domain of MTP addresses (or locations) reachable by the STP based on the provisioned Ordered Route relationships in the STP. As a generalization, the Destination entity plays various roles in the STP data model to represent the physical and logical MTP locations such as SPs, Clusters, and Capability Group.

**Key Attribute(s):** destination_address

**Other Attributes:**  
- destination_id
- mtp_loop_test_condition
- xudt_capability_indicator
  (This entity may have supplier specific additional attributes.)

**Relationships:** Ordered Route
**Entity Name:** Existing Translation Type  
**Entity Type:** Subtype of “Translation Type” entity  
**Description:** *Existing Translation Type* is the entity set that indicates the Translation Types to be mapped by the *Translation Type Mapping* relationship to the *Mapped Translation Types* on an incoming or outgoing SS7 message basis for a specific *Gateway Link Set*.

**Key Attribute(s):** translation_type  
**Other Attributes:** none  
**Relationships:** Translation Type Mapping

**Entity Name:** Foreign SP  
**Entity Type:** Role of SP entity  
**Description:** *Foreign SP* is an entity set that represents various types of CCS Signaling Points (SP) that belong to ICNs. These SPs must be known to the Bcc in order to send CCS messages.

**Key Attribute(s):** clli  
**Other Attributes:** primary_point_code (It might be a key attribute)  
point_code  
**Relationships:** Gateway Link Set  
ICN PC Translating

**Entity Name:** Gateway Link Set  
**Entity Type:** Role of Link Set associative entity  
**Description:** The *Gateway Link Set* entity set identifies a set of links that connects the STP to the adjacent SPs in another CCS network. (See *Link Set* for more details about Link Sets)

**Key Attribute(s):** link_set_name  
**Other Attributes:** far-end_clli  
link_set_type  
number_of_assigned_links  
(This entity may have supplier specific attributes in addition to the attributes defined here.)  
**Relationships:** Ordered Route  
Translation Type Mapping
**Entity Name:** Gateway Link Set Group  
**Entity Type:** Superset Entity  
**Description:** The *Gateway Link Set Group* entity represents one or more *Gateway Link Sets* terminating at the STP that are associated with the common SCCP screening data (i.e., they participate in various common SCCP screening relationships) for multiple interconnected CCS networks.  
**Key Attribute(s):** gateway_link_set_group_id  
**Other Attributes:** none  
**Relationships:** SCCP Management Screening Criteria, TCAP Query Screening Criteria, TCAP Response Screening Criteria, Unitdata Service Screening Criteria

**Entity Name:** Global Title  
**Entity Type:** Associative Entity  
(See the STP Relationship data dictionary for more details.)

**Entity Name:** Global Title Address  
**Entity Type:** Regular Entity  
**Description** *Global Title Address* entity set identifies the provisioned global title addresses in the STP which are necessary for the global title translation of received SS7 messages.  
**Key Attribute(s):** global_title_address  
**Other Attributes:** none  
**Relationships:** Global Title
Entity Name: ICN (Interconnected CCS Network)
Entity Type: Regular entity
Description: The ICN entity set identifies the CCS networks that interconnected with the Bcc’s CCS network.
Key Attribute(s): cic
Alternate Key(s): NI + NC (see point_code)
Other Attributes: (Other ICN attributes (e.g., icn_name) may be required by the CCS operations for administrative purposes)
Relationships: ICN PC Translating

Entity Name: Link Set
Entity Type: Associative Entity
(see Link Set relationship in Relationship Dictionary)
Description: The Link Set associative entity identifies a set of links that connects the STP to the adjacent SPs. A link set is the collection of up to 16 signaling links that connect the STP to other adjacent signaling nodes. Assigning the “far-end clli” attribute to the Link Set creates a relationship over this entity between the Adjacent SP entity and the STP entity.
Key Attribute(s): link_set_name
Other Attributes: far_end_clli
link_set_type
number_of_assigned_links
five_to_eight_bit_SLS_mapping_indicator
link_set_internetwork_broadcast_indicator
min_tfr_broadcast_link_quantity
(This entity may have supplier specific attributes in addition to the attributes identified here.)
Relationships: Ordered Route

Entity Name: Link
Entity Type: Member Entity of Link Set
Description: The Link entity set identifies the characteristics of transmission paths between two CCS nodes in the signaling network.
Key Attribute(s): link_set_name + link_member
Other Attributes:  
link_service_state  
link_speed  
enryption_option  
(In addition to the attributes given below, supplier specific attributes may be assigned to the Link entity.)

Relationships:  
Link Termination

Entity Name:  
Mapped Translation Type

Entity Type:  
Subtype of “Translation Type” entity

Description:  
Mapped Translation Type is the entity set that indicates the valid Translation Types to be used by the CCS network providers independent from each other. The externally used Translation Types are converted to the valid Translation Types, which are indicated by this entity, used internally by the Bcc. Similarly, the internally used Translation Types are converted to the valid Translation Types which are externally valid in the interconnected CCS Network.

Key Attribute(s):  
translation_type

Other Attributes:  
none

Relationships:  
Translation Type Mapping

Entity Name:  
MTP Message Type

Entity Type:  
Dependent Entity on Allowed SIO

Description:  
The MTP Message Type entity identifies the specific types of MTP NM and T&M messages to be screened according to MTP NM Screening Criteria and MTP T&M Screening Criteria relationships.

Key Attribute(s):  
allowed_sio + h0_header_code + h1_header_code

Other Attributes:  
none

Relationships:  
MTP NM Screening Criteria  
MTP T&M Screening Criteria

Entity Name:  
Ordered Route

Entity Type:  
Associative Entity (See the STP Relationship data dictionary for more details.)

Entity Name:  
Port
**Entity Type:** Regular Entity

**Description:** The *Port* entity set identifies the STP’s termination points for SS7 signaling links. It represents the set of assignable hardware ports and their current provisioning status.

**Key Attribute:** port_location

**Other Attributes:**
- port_state
- equipment_type
- equipment_options
  
  *(There might be supplier specific additional attributes)*

**Relationships:** Link Termination

**Entity Name:** Remote SP

**Entity Type:** Role of SP entity

**Description:** *Remote SP* is an entity set that represents various types of CCS nodes that have no *Link Sets* terminating at the STP.

**Key Attribute(s):** clli

**Other Attributes:**
- point_code

**Relationships:** Ordered Route

**Entity Name:** SCCP Application

**Entity Type:** Superset Entity of SCP Application and SSP Application

**Description:** As a generalization of the *SCP Application* and *SSP Application* entities, the *SCCP Application* entity set indicates the CCS nodes where the specific CCS service applications reside.

**Key Attribute(s):** node_application_address

**Other Attributes:**
- signaling_point_status
- subsystem_status
- isni_capability_indicator

**Relationships:** Ordered GTT
Concerned Signaling Points
Entity Name: **SCCP Destination**

**Entity Type:** Superset Entity

**Description:** As a generalization of the **SCCP Application** and **Capability Group** entities, the **SCCP Destination** entity indicates the provisioned results of possible global title translations in STP based on the **Ordered GTT** relationship. A global title translation process in STP produces either a node application location (i.e., a **SCCP Application** entity) or another STP address (i.e., a **Capability Group** entity) where another global title translation will be performed.

**Key Attribute(s):** sccp_destination_address

**Other Attributes:** none

**Relationships:** Ordered GTT

Entity Name: **SCCP Management Message Type**

**Entity Type:** Dependent Entity on Allowed SIO

**Description:** **SCCP Message Type** is an entity that identifies the specific types of **SCCP Management** messages to be screened according to the **SCCP Management Screening Criteria** relationship.

**Key Attribute(s):** allowed_sio + scmg_format_id

**Other Attributes:** none

**Relationships:** SCCP Management Screening Criteria

Entity Name: **SCP (Service Control Point)**

**Entity Type:** Subtype of SEP entity

**Description:** **SCP** is an entity set that represents the CCS service control platforms which interacts with the STP in order to provide (and control) CCS based services.

**Key Attribute(s):** clli

**Other Attributes:** point_code

**Relationships:** Ordered Route

Entity Name: **SCP Application**

**Entity Type:** Dependent Entity on SCP
**Description:** SCP Application entity represents the CCS based services provided by the CCS network provider via SCPs.

**Key Attribute(s):** scp_application_address

**Other Attributes:** alternate_routing_on_congestion_indicator

(This entity may have additional attributes such as “scp_application_name,” “scp_application_version” that will be of interest to the CCS service data administration.)

**Relationships:** Concerned Signaling Points
SCP Application Mating

---

**Entity Name:** SEP (Signaling End Point)

**Entity Type:** Subtype of Destination Entity

**Description** As a generalization of the CCSSO, SCP, and STP entities, the SEP entity set represents various types of SPs (except STPs) which interact with the STP in the CCS network.

**Key Attribute(s):** clli

**Other Attributes:** point_code

**Relationships:** Ordered Route

---

**Entity Name:** SP (Signaling Point)

**Entity Type:** Subtype of Destination entity

**Description** As a generalization of the SEP and STP entities, SP is an entity set that represents various types of CCS nodes in the CCS network.

**Key Attribute(s):** clli

(For the interconnected CCS networks, the “clli” attribute for an SP may be null. If this is that case, “point_code” will be used an alternate key for those SPs.)

**Other Attributes:** point_code

**Relationships:** Ordered Route

---

**Entity Name:** SSP (Service Switching Point)

**Entity Type:** Subtype of SEP entity
**Description**
The SSP entity set represents all switching offices (and their remotes) that identify calls associated with intelligent network services and initiate dialogs with the SCPs (in which the service logics reside) via CCS network.

**Key Attribute(s):** clli

**Other Attributes:**
- primary_point_code
- number_of_point_codes
- point_code_list

**Relationships:** Ordered Route

**Entity Name:** SSP Application

**Entity Type:** Dependent Entity on SSP

**Description:** SSP Application entity set represents the CCS based services provided by the CCS network provider via SSPs.

**Key Attribute(s):** ssp_application_address

**Other Attributes:** (This entity may have additional attributes such as “ssp_application_name,” “ssp_application_version” that will be of interest to the CCS service data administration.)

**Relationships:** Concerned Signaling Points

**Entity Name:** STP (Signaling Transfer Point)

**Entity Type:** Subtype of SP Entity

**Description**
The STP entity set represents the STP (including its mate via STP Mating relationship) in a CCS network that relay SS7 messages from a origination SP to a destination SP.

**Key Attribute(s):** clli

**Other Attributes:**
- point_code
- capability_code
- cluster_code
- mtp_loop_test_indicator
- mtp_loop_test_message_quantity
- mtp_loop_message_sampling_quantity
- internetwork_broadcast_indicator
- periodic_slr_indicator
- tfa/tfr_pacing_rate
(There might be supplier specific attributes).
**Relationships:**
Ordered Route  
STP Mating  
Link Set (Associative Entity)

**Entity Name:** Translation Type  
**Entity Type:** Superset Entity  
**Description:** As a generalization of the Existing Translation Type and Mapped Translation Type entities, the Translation Type entity set represents the provisioned data together with the Global Title Addresses to constitute the valid Global Titles of the received SS7 messages.

**Key Attribute(s):** translation_type  
**Other Attributes:** none  
**Relationships:**  
Global Title (with Global Title Address)  
Translations Type Mapping (with Mapped Translation Type and Existing Translation Type roles)

**5.2.3.4 STP Relationship Data Dictionary**

**Relationship Name:** Concerned Signaling Points  
**Relationship Description:** This relationship indicates the specific SP to be informed when the subsystem of a specific application becomes unavailable (or available after being unavailable for a while).

**Key Attribute(s):** node_application_address  
**Other Attributes:** concerned_point_codes  
**Relationship Cardinality:** SP (1,N):(1,1) SCCP Application

**Relationship Name:** Global Title (Associative Entity)  
**Description** The Global Title is the relationship that is provisioned by associating the Global Title Address and Translation Type entities to perform global title translation processes in the STP for received SS7 messages.

**Key Attribute(s):** translation_type + global_title_address  
**Other Attributes:** none
**Relationship Cardinality:** Translation Type (1,N):(1,M) Global Title Address

**Relationship Name:** ICN PC Translating

**Relationship Description:** This relationship indicates the possible PCs that belong to a specific ICN to route the TCAP messages when ICN Based Treatment is in effect. The priority of the PC choice is always indicated by relative_cost attribute if there are multiple PCs involved for a given ICN.

**Key Attribute(s):** cic + point_code

**Other Attributes:** icn_routing_relative_cost

**Relationship Cardinality:** ICN (1,1):(1,N) Foreign STP

**Relationship Name:** ISDNUP (ISDN User Part) Message Type Screening Criteria

**Description** ISDNUP Message Type Screening Criteria is a relationship that defines the provisioned gateway screening data for the screening process of ISDNUP messages received from a Gateway Link Set.

**Key Attribute(s):** gateway_link_set_name + allowed_opc + blocked_opc + allowed_sio + allowed_dpc + blocked_dpc + allowed_isupmt

**Other Attributes:** screening_outcome

**Relationship Cardinality:** Gateway Link Set (1,M):(0,M) Allowed OPC, (0,M) Blocked OPC, (1,M) Allowed SIO, (0,M) Allowed DPC, (0,M) Blocked DPC, (0,M) Allowed ISDNUP Message Type

**Relationship Name:** Link Set (an Associative Entity)

**Relationship Description:** (see the Link Set associative entity in Entity Dictionary)

**Key Attribute(s):** (see the Link Set associative entity in Entity Dictionary)

**Other Attributes:** (see the Link Set associative entity in Entity Dictionary)

**Relationship Cardinality:** Adjacent SP (1,1):(1,1) STP
Relationship Name: Link Termination

Relationship Description: The Link Termination relationship identifies the port assignment of each Link at the STP.

Key Attribute(s): link_set_name + link_member + port_location

Other Attributes: none.

Relationship Cardinality: Port (0,1):(0,1) Link

Relationship Name: MTP Loop Testing (Relationship)

Relationship Description: This relationship indicates the specific Remote SP to be tested for a particular cluster for MTP loops when triggered by a routing change at the STP. The default case will be the Remote SP with a network cluster member number of 1 will be the SP to be tested for a cluster.

Key Attribute(s): destination address + point_code

Other Attributes: none

Relationship Cardinality: Cluster (0,1):(0,1) Remote SP

Relationship Name: MTP-NM (MTP Network Management) Screening Criteria

Description: MTP-NM Screening Criteria is a relationship that defines the provisioned gateway screening data for the screening process of MTP-NM messages received from a Gateway Link Set. The message_priority and service_indicator parts of “allowed_sio” attribute and the participation of MTP Message Type entity in this relationship should clearly indicate that the screened messages are the MTP-NM messages.

Key Attribute(s): gateway_link_set_name + mtp_message_type + allowed_opc + blocked_opc + allowed_sio + h0_header_code + h1_header_code + allowed_dpc + blocked_dpc + allowed_affected_destination

Other Attributes: screening_outcome

Relationship Cardinality: Gateway Link Set (1,N):(1,M) MTP Message Type,(0,M) Allowed OPC, (0,M) Blocked OPC, (1,M) Allowed SIO, (0,M) Allowed DPC, (0,1) Blocked DPC, (1,M) Allowed Affected Destination
Relationship Name: MTP-T&M (MTP-Testing & Maintenance) Screening Criteria

Description: MTP-T&M Screening Criteria is a relationship that defines the provisioned gateway screening data for the screening process of MTP-T&M messages received from a Gateway Link Set. The message_priority and service-indicator parts of “allowed_sio” attribute and the participation of MTP Message Type entity should clearly indicate that the screened messages are the MTP-T&M messages.

Key Attribute(s): gateway_link_set_name + allowed_opc + blocked_opc + allowed_sio + h0_header_code + h1_header_code + allowed_dpc + blocked_dpc

Other Attributes: screening_outcome

Relationship Cardinality: Gateway Link Set (1,N):(1,M) MTP Message Type,(0,M) Allowed OPC, (0,M) Blocked OPC, (1,M) Allowed SIO, (0,M) Allowed DPC, (0,M) Blocked DPC,

Relationship Name: Ordered GTT (Global Title Translation)

Relationship Description: The Ordered Global Title Translation relationship represents the provisioned address translations in the STP to derive the SCCP Destination from the Global Titles provided by the received SS7 messages. (This relationship also serves as an entity (i.e., an Associative Entity) in the STP data model.)

Key Attribute(s): translation_type + global_title_address + sccp_destination

Other Attributes: gtt_relative_cost routing_indicator

Relationship Cardinality: Global Title Address (1,N):(1,1) SCCP Destination

Relationship Name: Ordered Route

Relationship Description: The Ordered Route relationship represents the specific MTP routing instructions that are provisioned for sending the SS7 messages to specific Destinations by selecting specific Link Sets.

Key Attribute(s): link_set_name + destination_address
Other Attributes:  route_relative_cost  
route_status  

Relationship Cardinality:  Link Set (1,N):(1,1) Destination, (0,M) STP

Relationship Name:  SCCP-MGT (SCCP Management) Screening Criteria
Description:  SCCP-MGT Screening Criteria is a relationship that defines the provisioned gateway screening data for the screening process of SCCP MGT messages received from a Gateway Link Set.
Key Attribute(s):  gateway_link_set_name + gateway_link_set_group_id + allowed_opc + blocked_opc + allowed_sio + allowed_dpc + blocked_dpc + allowed_cgpa + affected_pc_ssn
Other Attributes:  screening_outcome  

Relationship Cardinality:  Gateway Link Set (1,N):(0,M) Gateway Link Set Group, (0,M) Allowed OPC, (0,M) Blocked OPC, (1,M) Allowed SIO, (0,M) Allowed DPC, (0,M) Blocked DPC, (0,M) Allowed CGPA, (0,M) Allowed CDPA, (1,M) Allowed Affected PC/SSN

Relationship Name:  SCP Application Mating
Relationship Description:  Since the deployment of some CCS service applications may require a distributed service configuration with multiple SCPs for load balancing and backup purposes, the SCP Application Mating relationship identifies the mates of a specific SCP application in the CCS network.
Key Attribute(s):  scp_application_address + scp_application_address
Other Attributes:  none  
Relationship Cardinality:  SCP Application (0,N): (0,M) SCP Application

Relationship Name:  STP Mating
Relationship Description:  This relationship indicates the STP mate configuration
Key Attribute(s):  point_code + point_code (or clli + clli)
Other Attributes:  none
Relationship Cardinality: STP (1,1): (1,1) STP

Relationship Name: TCAP (Transaction Capabilities Application Part) Query Screening Criteria

Description: TCAP Query Screening Criteria is a relationship that defines the provisioned gateway screening data for the screening process of TCAP Query messages received from a Gateway Link Set.

Key Attribute(s): gateway_link_set_name + gateway_link_set_group_id + allowed_opc + blocked_opc + allowed_sio + allowed_dpc + blocked_dpc + allowed_cgpa + allowed_tt + allowed_cdpa

Other Attributes: screening_outcome

Relationships: Gateway Link Set (1,N):(0,M) Gateway Link Set Group, (0,M) Allowed OPC, (0,M) Blocked OPC, (1,M) Allowed SIO, (0,M) Allowed DPC, (0,M) Blocked DPC, (0,M) Allowed CGPA, (1,M) Translation Type, (0,M) Allowed CDPA

Relationship Name: TCAP Response Screening Criteria

Description: TCAP Response Screening Criteria is a relationship that defines the provisioned gateway screening data for the screening process of TCAP Response messages received from a Gateway Link Set.

Key Attribute(s): gateway_link_set_name + gateway_link_set_group_id + allowed_opc + blocked_opc + allowed_sio + allowed_dpc + blocked_dpc + allowed_cgpa + allowed_cdpa

Other Attributes: screening_outcome

Relationship Cardinality: Gateway Link Set (1,N):(0,M) Gateway Link Set Group, (0,M) Allowed OPC, (0,M) Blocked OPC, (1,M) Allowed SIO, (0,M) Allowed DPC, (0,M) Blocked DPC, (0,M) Allowed CGPA, (0,M) Allowed CDPA

Relationship Name: Translation Type Mapping
Relationship Description: This relationship indicates that some Translations Types used by the external CCS network providers must be mapped to internally used Translation Types (and vice versa) per Gateway Link Set basis.

Key Attribute(s): translation_type + gateway_link_set_name + incoming_outgoing_indicator

Other Attributes: none

Relationship Cardinality: Mapped Translation Type (1,1):(1,1) Existing Translation Type, (1,1) Gateway Link Set

Relationship Name: Unitdata Service Screening Criteria

Description: Unitdata Service Screening Criteria is a relationship that defines the provisioned gateway screening data for the screening process of Unitdata Service messages received from a Gateway Link Set.

Key Attribute(s): gateway_link_set_name + gateway_link_set_group_id + allowed_opc + blocked_opc + allowed_sio + allowed_dpc + blocked_dpc + allowed_cgpa allowed_cdpa

Other Attributes: screening_outcome

Relationship Cardinality: Gateway Link Set (1,N):(0,M) Gateway Link Set Group, (0,M) Allowed OPC, (0,M) Blocked OPC, (1,M) Allowed SIO, (0,M) Allowed DPC, (0,M) Blocked DPC, (0,M) Allowed CGPA, (0,M) Allowed CDPA

5.2.3.5 STP Attribute Data Dictionary

As part of the attribute definitions, the following notation are used to define the format of each attribute:

- A(x) - meaning an alphabetic ASCII character string having at most x characters.
- BIN(x) - meaning a binary character string having at most x characters.
- N(x) - meaning an ASCII numeric character string of up to x characters.
- AN/G(x) - meaning an ASCII character string containing up to x alphanumeric and graphic characters. Unless otherwise specified, each character may have any value in the subset of ASCII as discussed in TA-STS-000298, Signal Transfer Point/SEAS and
**Service Control Point/Service Management System Data Communication Interface Protocol Specification.** The attribute’s description may further restrict its format.

- **N/G(x)** - meaning an ASCII character string containing up to x numeric and graphic characters.

**allowed_affected_destination:** N(9); this attribute as an alias identifies the destination_address of specific destination that is experiencing failure or congestion. (See destination_address)

**allowed_affected_pc_ssn:** N(12); the point_code and/or subsystem_number of the SP that is experiencing failure or congestion. (See point_code and subsystem_number)

**allowed_edpa:** Called Party Address in general can be a Global Title (global_title_address + translation_type) or a point_code and/or a subsystem_number. It is a variable parameter. This attribute indicates the Called Party address that is allowable for received SS7 messages to pass the gateway screening process at the STP. (See global_title_address, translation_type, point_code and subsystem_number)

**allowed_egpa:** Calling Party Address, like Called Party Address, can be a Global Title (global_title_address + translation_type) or a point_code and/or a subsystem_number. It is a variable parameter. This attribute indicates the Called Party address that is allowable for received SS7 messages to pass the gateway screening process at the STP. (See global_title_address, translation_type, point_code and subsystem_number)

**allowed_dpc:** N(9); this attribute identifies the point_code of a specific Signaling Point as an alias. (See point_code)

**allowed_isupmt:** N(3); this attribute identifies decimal representation of the ISDNUP message types that are allowed to pass the gateway screening process at the STP.

**allowed_opc:** N(9); this attribute identifies point_code of a specific Signaling Point as an alias (See point_code).

**allowed_sio:** The Signaling Information Octet (SIO) is the concatenation of the following subfields:

- **service indicator:** two numeric characters with allowable value set of [00-15]
- **network indicator code:** one numeric character with allowable value set of [0,1,2,3]
- **message priority:** one numeric character with allowable value set of [0,1,2,3]

This attribute defines SIO value that is allowable for received SS7 messages to pass the gateway screening process at the STP.
allowed_tt: N(3); this attribute identifies (as an alias) the allowable translation_types for received SS7 messages to pass the gateway screening process at the STP (See translation_type).

alternate_routing_on_congestion_indicator: BIN(1); indicates whether the alternate routing on congestion is permitted by the SCP Application. A value of 0 indicates that the alternate routing on congestion is not permitted and a value of 1 means that the alternate routing on congestion is permitted. The value of 0 shall be the default value.

blocked_dpc: N(9); this attribute identifies the point_code of a specific Signaling Point as an alias. (See point_code).

blocked_opc: N(9); this attribute identifies the point_code as an alias. (See point_code)

capability_code: N(9), fixed length; this attribute identifies a group of functionally related STPs in the signaling network. For example, it may refer to a given service-related SCCP capability resident at that STP (e.g., the ability to perform global title translations for a given translation type). From the perspective of the internal protocol, each occurrence of this attribute is to be treated as the STP’s signaling point code for MTP message discrimination and routing purposes. This attribute has the same format of point_code attribute. (See point_code)

cic: N(4), fixed length; the ICN routing identifier in Carrier Identification-CIC format identifying the End User’s Presubscribed Interexchange Carrier (EUPIC) that would be used to route the SS7 message. Valid codes are 0000 through 9999.

clli: A/N(11), fixed length; the COMMON LANGUAGE® CLLI™ code is an attribute that uniquely identifies the SPs in terms of its physical location. It is comprised of concatenated subfields such as city (or locality), state (or province), building, and traffic unit identity. More specifically, its format is:

cccscssbbuuu,

where

ccc  denotes a 4-character city, town, or locality code,
ss   denotes a two-character state or province code,
bb   denotes a two-character building code, and
uuu  denotes a three-character traffic unit identifier that uniquely identifies the STP at the physical location.

cluster_code: N(6), fixed length; this attribute defines the destination_address of a cluster. It is formed by the concatenation of Network Identifier and Network Cluster subfields of the point_code attribute format.

COMMON LANGUAGE is a registered trademark, and CLEI, CLFI, CLLI, and CLCI are trademarks of Bellcore.
concerned_point_codes: bN(x), variable length; a list of the point codes that contains “b” entries of the concerned signaling points which are to be notified. The format of this attribute is the same as the point_code attribute defined in this dictionary. Any number of concerned point codes may be specified. The number of concerned signaling points for a given application depends heavily on the particular application and CCS network configuration. (See point_code)

destination_address: N(9) or N(6), variable length; the SS7 network address identifying a signaling point or collection of signaling points to which the STP may route SS7 message traffic. The destination address may be an alias for:

- a nine-digit point_code defining a unique destination signaling point in the CCSN;
- a nine-digit capability_code uniquely defining a pair or collection of STPs supporting the same functional capabilities; or
- a six-digit cluster_code defining a collection of signaling points sharing the same network identifier (NI) code and network cluster (NC) code.

The destination address is formed by the concatenation of the base-10 (decimal) representations of the corresponding binary octets comprising the respective subfields of the SS7 signaling point code:

- the network identifier (NI) \{001, \ldots, 255\},
- the network cluster (NC) code \{001, \ldots, 255\}, and when applicable,
- the network cluster member (NCM) code \{000, \ldots, 255\}.

destination_id: N(x); this attribute is an alias for clli or an interconnected network specific destination location attribute. (See clli)

enumeration_option: A (1), (Y= Yes and N= No); this attribute determines whether or not the data on the link is encrypted.

equipment_options: A(10); this attribute provides a hardware (or software) to be set for the desired usage mode of the equipment. This attribute is currently a supplier-specific parameter.

far_end_clli: A/N(11), fixed length; as an alias for clli, this attribute identifies the clli of adjacent node at the far end of the link set.

five_to_eight_bit_SLS_mapping_indicator: BIN(1); indicates whether the five to eight bit SLS mapping feature should be done for messages being routed to this link set. A value of 0 indicates that these procedures are disabled for the link set. A value of 1 indicates that these procedures are enabled for the link set. The value of 0 shall be the default value.

gateway_link_set_group_id: N(2); this attribute provides an identifier for one or more link sets terminating at the STP. The link set group identifier is used to enable the use of common screening data for multiple interconnected networks while still being able to
identify the Calling Party Address Point Codes and SSN combinations that are allowed to transmit SCCP messages on specific incoming link sets.

**gateway_link_set_name:** A unique identifier for the Gateway Link Set. (See *link_set_name*)

**global_title_address:** A/N(10), variable length; the non-SS7 address transmitted to the STP for translation. For each translation type, the allowable length or lengths and allowable value set for the global title address must be defined.

**gtt_relative_cost:** N(2), fixed length; the weighting factor applied to the *Ordered Global Title Translation* relationship. The costs will be assigned values from 00 to 99, representing the most desirable to the least desirable, respectively. The translations of equal desirability are assigned equal costs.

For a given global title address, the least cost SS7 address (i.e., node_application_address) should be selected as the primary SS7 address. Alternate SS7 addresses are to be selected in the order of their increasing relative cost factors. Although current protocol standards and initial network architectures may support only mated-pair application configurations, the above scheme does not restrict the global title translation to a single alternate SS7 address. [Theoretically, up to 100 rank-ordered SS7 addresses for a given global title address may be specified with the two-digit relative cost factor.]

**h0_header_code:** N(2); together with h1_header_code, this attribute identifies a specific MTP Service Management message.

**h1_header_code:** N(2); together with h0_header_code, this attribute identifies a specific MTP Service Management message.

**icn_routing_relative_cost:** N(2); the weighting factor assigned to the ICN Routing Identifier and Routing Label DPC objects. The costs may be assigned values from 00 to 99, representing the most desirable to least desirable, respectively. Objects of equal desirability are assigned equal costs.

**incoming_ongoing_indicator:** A(1), fixed length; used by the STP to indicate whether the translation type mapping data provisioned for the gateway link set is for received on the link set or sent on the link set. The values are “I” for incoming and “O” outgoing.

**internetwork_broadcast_indicator:** BIN(1); indicates whether TFP/TCP and TFA/TCA messages should be broadcast across network boundaries. A value of 0 indicates that the broadcast is turned off across network boundaries. A value of 1 indicates that the broadcast is turned on across network boundaries. The value of 0 shall be the default value. Note, this item corresponds to a conditional requirement in Section 4.2.4.12.1.

**isni_capability_indicator:** BIN(1); indicates whether the application at the node supports the ISNI capability. A value of 0 indicates that the application does not support ISNI and a value of 1 means that the application does support ISNI. The value of 0 shall be the default value.

---

3. DPCs and SSNs assigned equal costs indicates SCCP loadsharing.
**link_member:** N(2), fixed length; the logical identification of the individual member link within the Link Set. The value of the number is the base-10 (decimal) equivalent of the binary signaling link code (SLC) used internally by the SS7 protocol to identify this link. This value may range from 00 through 15. The concatenation of the member number with the link set name uniquely identifies the link in the CCS network.

**link_set_internetwork_broadcast_indicator:** BIN(1); indicates whether TFP/TCP and TFA/TCA messages should be broadcast across this link set. A value of 0 indicates that the broadcast is turned off for this link set. A value of 1 indicates that the broadcast is turned on across this link set. The value of 0 shall be the default value for gateway link sets and 1 otherwise. Note, this item corresponds to a conditional requirement in Section 4.2.4.12.1.

**link_set_name:** A/N(8), fixed length; the unique identifier for the link set. It is represented by a COMMON LANGUAGE code called a Link Set Serial Number (LSSN). It is a unique designation comprised of one alphabetic character concatenated with one alphanumeric character and six numeric characters.

**link_set_type:** A(1), fixed length; an identification of the type of link set in terms of its relationship to the CCS network architecture. The currently defined value set for this attribute includes {A (access links), B (bridge links), C (cross-links), D (diagonal links), and E (links between the STP and a remote signaling end-point)}.

**link_speed:** N/G(4), variable length; the data transmission speed of the link in units of kilobits-per-second (kbps), assuming that the link speed is a provisionable equipment option. [Supported values currently assumed are 9.6, 19.2, 56, and 64 kbps. Other values may be supported in the future.]

**link_service_state:** A(3), fixed length; describes the service status of the link as indicated below.

- **ACT** = Active: the link is in service and can be used to carry signaling traffic.
- **OOS** = Out of Service: the link is currently out of service but can be made active by the STP.
- **UAV** = Unavailable: the link is not available for use by the STP. It has been disabled by local or centralized maintenance personnel. This is a state which cannot be automatically overridden by the STP.

**min_tfr_broadcast_link_quantity:** N(2); indicates the minimum number of links that must be available in order for an STP to consider the route corresponding to a (combined) link set unrestricted.

**mtp_loop_message_sampling_quantity:** N(3); indicates the number of messages that are to be sampled for MTP loop detection when triggered upon congestion. Allowable range is 50 to 200. This attribute is referred to as parameter N in Section 2.4 in T1.111.7 of GR-246-CORE.
**mtp_loop_test_condition**: A(1); indicates whether the destination is to be tested for MTP loops upon provisioned routing changes or routing status changes.

- **N**: No testing based on routing change: do not perform a MTP loop detection test upon provisioned routing changes or routing status changes for this destination, or
- **P**: test on Provisioned routing changes for this destination, or
- **R**: test on Routing status changes for this destination, or
- **B**: Test on Both cases: perform a MTP loop detection test upon provisioned routing changes and/or routing status changes for this destination. This is the default.

**mtp_loop_test_indicator**: BIN(1); indicates whether the MTP loop detection procedures are enabled or disabled at the STP. A value of 0 indicates that the MTP loop detection procedures are disabled at the STP. A value of 1 indicates that the MTP loop detection procedures are enabled at the STP. The value of 1 shall be the default value.

**mtp_loop_test_message_quantity**: N(3); indicates the number of most frequently occurring DPCs that the MTP loop test messages are to be sent to when an MTP loop test is triggered upon congestion. The most frequent DPCs are determined from the mtp_loop_message_sampling_quantity of messages that have been sampled. Allowable range is 3 to 10. This attribute is referred to as parameter M in Section 2.4 in T1.111.7 of GR-246-CORE.

**mtp_restart_indicator**: BIN(1); indicates whether MTP restart should be performed upon node recovery. A value of 0 indicates that MTP restart should not be performed upon node recovery. A value of 1 indicates that the node should perform the restarting node procedures upon node recovery. Note that this parameter has no effect on the adjacent node procedures.

**network_cluster_exception_list_exclusion_indicator**: A(1); an indicator conveying whether the STP shall maintain a dynamic status exception list (x-list) for each cluster route that may be used to reach the member signaling points comprising that cluster. The x-lists shall be maintained on a per-route basis for each cluster, but shall be allowed or excluded on a per-cluster basis. Allowable arguments are

- **Y**: yes: exclude (do not maintain) exception lists for this cluster destination.
- **N**: no: normally include (maintain) status exception lists (x-lists) for this cluster destination (default).

**network_cluster_broadcast_exception_indicator**: A(1); an indicator conveying whether the STP should broadcast transfer prohibited (TFP), transfer allowed (TFA), transfer cluster prohibited (TCP), and transfer cluster allowed (TCA) MTP-NM status messages about the indicated network cluster destination address and any member signaling points in that cluster on its x-lists, to adjacent signaling points. Allowable arguments are

- **Y**: yes: (exception) do not broadcast transfer messages for this network cluster.
— N - no: (no exception) normally broadcast transfer messages for this network cluster (default).

**node_application_address**: N(12), fixed length; this is a composite attribute as the concatenation of **point_code** and **subsystem_number** attributes. (See **point_code** and **subsystem_number**)

**number_of_links**: N(2), variable length; the number of currently assigned link members comprising the link set. This attribute may take on integer values ranging from 0 to 16.

**number_of_point_codes**: N(1), fixed length; the number of **point_codes** that are assigned to CCSSO or SSP.

**periodic_slt_indicator**: BIN(1); indicates whether the periodic SLT procedures are enabled or disabled at the STP. A value of 0 indicates that the periodic SLT procedures are disabled at the STP. A value of 1 indicates that the periodic SLT procedures are enabled at the STP. The value of 1 shall be the default value.

**primary_point_code**: N(9), fixed length; an alias for **point_code** that identifies the primary address of multiple point code assigned Signaling End Points such as CCSSO or SSP.

**point_code**: N(9), fixed length; the network address used by the SS7 protocol to uniquely identify the STP. This attribute is formed by the concatenation of the three base-10 (decimal) representations of the corresponding binary octets comprising the network identifier (NI), network cluster (NC), and network cluster member (NCM) subfields of the internally stored binary signaling point code. Allowable values for the respective signaling point code subfields are:

<table>
<thead>
<tr>
<th>Subfield</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NI</td>
<td>001 - 255</td>
</tr>
<tr>
<td>NC</td>
<td>001 - 255</td>
</tr>
<tr>
<td>NCM</td>
<td>000 - 255</td>
</tr>
</tbody>
</table>

**point_code_list**: N(9), variable length; a list of secondary **point codes** associated with Signaling End Points such as CCSSOs or SSPs.

**port_location**: AN/G(16); the designation of where the appearance of a signaling link may be found physically on an STP. The specific format of this attribute is currently supplier-specific. Usage of the format described in the LSSGR is desirable.

**port_state**: A(1); the identification of the state of the port as indicated below:

- U= unequipped; not ready for assignment to a signaling link
- E= equipped but not assigned to a signaling link
- A= assigned; in service on a signaling link

**routing_indicator**: A(1), fixed length; This attribute specifies the value to be placed in the Message Signal Unit’s (MSU’s) binary Routing Indicator Bit following the translation
based on *Ordered Global Title Translation* relationship. That value conveys whether the MSU is to be routed entirely on the destination (DPC-SSN) provided in the translation or that a subsequent GTT will be required for the MSU at the provided destination and possibly at subsequent STPs as it traverses its path through the CCS network. The use of this attribute as a variable parameter is intended to support multiple (i.e., successive) global title translations for a given MSU in the course of its routing to its intended final destination signaling point.

The *routing_indicator* attribute will be considered a one-character alphabetic field containing one of the following values:

- **G** denotes the STP should place the value 0 in the MSU’s Routing Indicator Bit, conveying Global Title routing following the Global Title Translation (GTT); i.e., a subsequent GTT is needed for the message at the indicated destination.

- **D** denotes the STP should place the value 1 in the MSU’s Routing Indicator Bit, conveying Destination Point Code Routing following the GTT; i.e., no further GTTs are needed for the message.

In an *Ordered Global Title Translation* relationship for messages requiring further GTTs, the routing indicator argument of “G” will be specified, along with an SSN value of 000, denoting the “null” subsystem number at the target STP that is to perform the subsequent GTT.

The above implies that the STP will in fact support a variable reset action for the Routing Indicator Bit following a GTT.

**route_relative_cost:** N(2), fixed length; the weighting factor assigned to the link set as a route to the given destination. The costs may be assigned values from 00 to 99, representing the most desirable to least desirable, respectively. Routes of equal desirability for a given destination are assigned equal costs. Routes (i.e., link sets) to a given destination with differing costs correspond to the primary and alternate routes for that destination. The lowest-cost route is the primary route. Alternate routes are to be selected in the order of their increasing relative cost factors. Although at least two routes must be specified for each destination, given current network architecture requirements, the scheme described here does not restrict traffic for a given destination to a single alternate route. [Theoretically, up to 100 rank-ordered routes for a given destination may be specified with a two-digit relative cost factor.]

**route_set_status:** A(3), fixed length; the current availability status of the route set to the indicated destination as monitored by the STP’s internal SS7 signaling route management procedures. This attribute is not user-provisionable, but rather reflects a real-time status indication that is subject to change with network conditions. Allowable values are:

- **AVB** available
- **UAV** unavailable
CG1 congested - level 1
CG2 congested - level 2
CG3 congested - level 3
UAM unavailable due to MTP loop test.

route_status: A(4), fixed length, required; the current availability status of the route as monitored by the STP’s internal SS7 signaling route management procedures. This attribute is not user-provisionable, but rather reflects a real-time status indication that is subject to change with network conditions. Allowable values are:

- ALWD allowed
- RSTD restricted
- PRHB prohibited
- PRML prohibited due to MTP Loop detection.

sccp_destination_address: N(9) or N(12), fixed length; this attribute is an alias for capability_code or node_application_address. (See capability_code and node_application_address)

scp_application_address: N(12), fixed length; this is a composite attribute as the concatenation of point_code and subsystem_number attributes. (See point_code and subsystem_number)

scmg_format_id: N(3), fixed length, value range 001-255; this attribute identifies a specific SCCP Management Message.

screening_outcome: A(1), fixed length; the desired outcome of the gateway screening process. The STP can allow the message to be passed, fail the message, or to fail the message and not report it (i.e., to ignore it.). Allowable values are:

- A Allowed - Allow message into network
- F Fail - Do not allow message into network and report the rejection
- I Ignore - Do not allow message into network and do not report the rejection

signaling_point_status: A(4), fixed length; the SCCP status for the signaling point (at which the application resides) in terms of the STP’s ability to route message traffic to that signaling point. The SCCP maintains this status based on the receipt of MTP-STATUS, MTP-PAUSE and MTP-RESUME primitives (interlayer messages) from the STP’s MTP procedures, which monitor the status of the signaling route set used to reach the destination. Allowable values are:

- ALWD allowed
- PRHB prohibited
CG1 congested - level 1
CG2 congested - level 2
CG3 congested - level 3.

This attribute is not user-provisionable, but rather reflects a real-time status indication that is subject to change with network conditions.

**ssp_application_address**: N(12), fixed length; this is a composite attribute as the concatenation of *point_code* and *subsystem_number* attributes. (See *point_code* and *subsystem_number*)

**subsystem_number**: N(3), fixed length; the identification of the specific application subsystem at a signaling point. This Subsystem Number (SSN) attribute is comprised of the base-10 (decimal) representation of the binary number in the one-byte SSN used in the SS7 protocol. Allowable values range from 000, 002 through 255. [The value 001 is reserved for SCCP management]

**subsystem_status**: A(4), fixed length; the SCCP’s current status indication for the specific application subsystem at the indicated signaling point. The SCCP procedures maintain this status information based on the receipt of SCCP management subsystem-prohibited (SSP) and subsystem-allowed (SSA) messages. Allowable values are:

- ALWD allowed
- PRHB prohibited.

Subsystem status will also be marked prohibited by the STP whenever the signaling point status of the signaling point hosting the application is prohibited. Analogous to signaling point status above, this attribute is not user provisionable, but rather reflects a real-time status indication that is subject to change with network conditions.

**tfa/tfr_pacing_rate**: N(1); indicates the pacing rate for pacing TFA/TFR messages, when pacing is appropriate. The value is in tenths of seconds, and the range is 0 to 1 second. The value of 1 second shall be the default value.

**translation_type**: N(3), fixed length; identifies the type of global title translation. This attribute is the base-10 (decimal) representation of the 1-octet binary field used in the SS7 protocol to identify the translation type (001-254).

**xudt_capability_indicator**: BIN(1); indicates whether the node supports the XUDT capability. A value of 0 indicates that the node does not support XUDT and a value of 1 means that the node does support XUDT. The value of 0 shall be the default value.
5.2.3.6   STP Database Updates and Data Operations

R5-13   [313] The STP shall provide all necessary database capabilities for the
users to update or verify the data in the STP database (user data view)
based on the STP data model.

The users may issue RC requests containing STP database updates whose actual
implementations are intentionally deferred to a later time by the users. These requests are
referred to as “delayed RC orders.”

R5-14   [314] The STP shall be able to perform all necessary operations on
administrative data including the following list. In this list, a dagger (†) indicates these messages may be implementation-specific and are not
directly supported by the SEAS System; an asterisk (*) indicates that with
the addition of the Multi-Step GTT messages, this message is no longer
needed. However, this message will be “grandfathered” in case previous
implementations need it.

…
… A. RC COMMANDS
…
… • Activate a Delayed Order
… • Delete a Delayed Order
… • Cancel Activation of a Delayed Order
… • Assign Self-Identification
… • Change Self-Identification
… • Add Link Sets
… • Delete Link Sets
… • Change Link Set Attributes
… • Add (Provision) Signaling Links
… • Delete (Disconnect) Signaling Links
… • Change Link Attributes
… • Add Equipment to Ports †
… • Delete Equipment from Ports†
… • Change Equipment Attributes of Ports†
… • Add Destination
… • Delete Destination
… • Change Destination Attributes
… • Assign Ordered Routes
… • Delete Ordered Routes
… • Change Ordered Routes
… • Add Ordered Global Title Translations*
… • Delete Ordered Global Title Translations*
… • Change Ordered Global Title Translations*
… • Add Multi-Step GTT: TT-to-SSN Translation
… • Delete Multi-Step GTT: TT-to-SSN Translation
… • Change Multi-Step GTT: TT-to-SSN Translation
… • Add Multi-Step GTT: GTA-to-DPC Translation
… • Delete Multi-Step GTT: GTA-to-DPC Translation
… • Change Multi-Step GTT: GTA-to-DPC Translation
… • Add Multi-Step GTT: Ordered DPC
… • Delete Multi-Step GTT: Ordered DPC
… • Change Multi-Step GTT: Ordered DPC
… • Assign Mate Applications*
… • Delete Mate Applications*
… • Change Mate Applications*
… • Add SCCP Application Data
… • Delete SCCP Application Data
… • Change SCCP Application Data
… • Assign Concerned SPs
… • Delete Concerned SPs
… • Change Concerned SPs
… • Update STP Options
… • Add an ISNI: ICN/DPC Identification (See E.7.1.3)
… • Delete an ISNI:ICN/DPC Identification
… • Change an ISNI:ICN/DPC Identification
… • Add an ISNI: CIC/ICN Identification (See E.7.1.3)
• Delete an ISNI: CIC/ICN Identification

• Change an ISNI: CIC/ICN Identification

[Note: the following messages are to be supported for Gateway STPs]

• Add a Gateway Link Set

• Delete a Gateway Link Set

• Change a Gateway Link Set

• Add an Allowed OPC

• Delete an Allowed OPC

• Change an Allowed OPC

• Add a Blocked OPC

• Delete a Blocked OPC

• Change a Blocked OPC

• Add an Allowed SIO

• Delete an Allowed SIO

• Change an Allowed SIO

• Add an Allowed DPC

• Delete an Allowed DPC

• Change an Allowed DPC

• Add a Blocked DPC

• Delete a Blocked DPC

• Change a Blocked DPC

• Add an Affected DESTFLD

• Delete an Affected DESTFLD

• Change an Affected DESTFLD

• Add an Allowed ISDNUP Message Type

• Delete an Allowed ISDNUP Message Type

• Change an Allowed ISDNUP Message Type

• Add an Allowed CGPA

• Delete an Allowed CGPA
... • Change an Allowed CGPA
... • Add an Allowed TT
... • Delete an Allowed TT
... • Change an Allowed TT
... • Add an Allowed CDPA
... • Delete an Allowed CDPA
... • Change an Allowed CDPA
... • Add an Affected PC/SSN
... • Delete an Affected PC/SSN
... • Change an Affected PC/SSN
... • Add Translation Type Mapping
... • Delete Translation Type Mapping
... • Change Translation Type Mapping

B. VERIFICATION COMMANDS

... • Verify Delayed Orders
... • Verify Self-identification
... • Verify Link Set Attributes
... • Verify Link Set Members
... • Verify Port
... • Verify Destination
... • Verify Ordered Routes
... • Verify Ordered Global Title Translations*
... • Verify Multi-Step GTT: TT-to-SSN Translation
... • Verify Multi-Step GTT: GTA-to-DPC Translation
... • Verify Multi-Step GTT: Ordered DPC
... • Verify Mate Applications*
... • Verify SCCP Application Data
... • Verify Concerned SPs
... • Verify STP Attributes
... • Verify an ISNI: CIC/ICN Identification
... • Verify an ISNI: ICN/DPC Identification
  \hspace{1cm} \textit{[Note: the following messages are to be supported for Gateway STPs]}
... • Verify a Gateway Link Set
... • Verify an Allowed OPC
... • Verify a Blocked OPC
... • Verify an Allowed SIO
... • Verify an Allowed DPC
... • Verify a Blocked DPC
... • Verify an Affected DESTFLD
... • Verify an Allowed ISDNUP Message Type
... • Verify an Allowed CGPA
... • Verify an Allowed TT
... • Verify an Allowed CDPA
... • Verify an Affected PC/SSN
... • Verify Translation Type Mapping

The RC&V commands are defined in the STP/SEAS system interface of GR-310-CORE and GR-778-CORE (for gateway STPs).

5.2.3.7 Integrity Constraint Specifications

\textbf{R5-15} \hspace{0.5cm} \textbf{[315]} The STP shall implement RC data integrity checks defined in GR-310-CORE. These checks should be applied to data entered via a work position or SEAS system interface.

Integrity checks defined in GR-310-CORE include the following validations:

- Domains for all attributes of every entity set
- Constraints among attribute values of the same entity set
- Constraints among attributes of different entity sets
- Constraints on combined values of attributes
- Restrictions among sets of attributes (e.g., subset and mutual exclusion constraints)
- Restrictions on the way that attribute values are allowed to change.
Examples of these constraints are that it shall not be possible to

- Add or assign an entity if the identified entity is already assigned
- Delete an entity unless the entity is already assigned
- Assign members to a link set unless the link set itself exists
- Delete a link set without first deleting all its member links.

**R5-16** [316] If one or more constraints are violated during a database initialization, reinitialization, bulk load, or update process, a diagnostic notification shall be sent to the user specifying the integrity constraints violated and the data in error. At this point, the process shall be prevented from updating the database.

### 5.2.3.8 User Views and Logical Data Model

Users of data convey their requirements for reviewing and updating specific data stored in a database by defining “User Views (UVs).” The UVs are used for developing user interfaces (e.g., data displays, data entry methods, etc.). The data specified for a UV may contain the attributes that belong to one or more entities or relationships from the Logical Data Model. The UVs may also contain some parameters such as a display page number (for multi-screen displays), menu icons, pointers to other UVs; which are not any concern of the Logical Data Model created for the enterprise. In this document, various UVs are specified in the appendix sections under the Memory Administration requirements subsection headings.

### 5.2.4 STP Database Management Functions

#### 5.2.4.1 Database Updates

**R5-17** [317] Both immediate and delayed activation of RC messages shall be possible. Recent changes should not take effect during any process that accesses the information being changed.

**R5-18** [318] RC messages shall be logged on an external device to facilitate database recovery.
5.2.4.2 Database Assembly

R5-19 [319] The STP supplier shall provide a capability for interactive initial database assembly at the STP. This capability may be integrated into the STP or supplied in a stand-alone system.

R5-20 [320] Instructions to aid the Bcc in the initial database assembly shall be furnished.

5.2.4.3 STP Database Backup

R5-21 [321] Database backup includes functions necessary for backing up the STP database. The STP shall have the capability of storing primary and secondary copies of the database in protected memory.

R5-22 [322] These guidelines must be met for database backup:

... • The user shall have the ability to schedule automated backup procedures.

... • The user shall be able to order the creation of backup copies of the database.

... • The current STP database shall not be destroyed or altered during “automatic” creation of a primary or secondary copy.

... • Service at the STP shall not be affected by the creation of database backups.

... • A new primary copy of the STP database shall be automatically created at least once every 24 hours.

... • Each copy must contain the date and time of creation.

R5-23 [323] The supplier shall provide capabilities to support the following database backup schemes.

... 1. The primary copy shall be copied to become the secondary copy.

... 2. The current STP database shall be copied to become the primary copy.

R5-24 [324] The STP shall be able to write copies of the current database and its backups to an external device. It shall be possible to restore the primary and secondary database copies from the copies written in the external device.
R5-25  [325] It shall be possible to write these external copies without interference with any other database activities.

5.2.4.4 Database Restoration

R5-26  [326] The STP database shall be restored automatically as part of the initialization or reinitialization process at the STP.

R5-27  [327] It shall be possible to restore the STP database from the most recent backup copy of the STP database in the STP or from an external copy. When the STP restores the database, it shall update it automatically with recent changes from the Recent Change Log.

R5-28  [328] The entire restoration process shall take less than 30 minutes.

5.2.4.5 System Initialization

R5-29  [329] If a system initialization alters or erases the STP database partially or totally, the database shall be automatically rebuilt by the database restoration routines.

5.2.4.6 System Growth

R5-30  [330] Hardware or software changes in the STP that do not affect the database shall be added without having to reinput the database.

R5-31  [331] If a hardware or a software generic change requires a rebuilt database, the supplier shall provide the means of converting the database from the old configuration to the new with minimal user manual intervention.

5.2.5 Memory Space Accounting

5.2.5.1 Background

Memory Space Accounting requires that the STP provide an accounting of the amount of memory space allocated to CCS translations, the amount used by existing CCS translations, and the available memory for new CCS translations.
The provisioned physical or logical CCS node resources, such as terminal equipment or 800-NXX codes, are inventoried to keep track of their availability for future assignments. However, the available memory spaces in CCS nodes for future CCS translations assignments were not considered to be a provisionable node resource to be tracked by the provisioning inventories. This becomes a problem when large numbers of translations are to be deployed during mass CCS node database updates if CCS nodes do not have the required memory space to fit those new translations. Users may then find out unexpectedly that they have run out of space in certain tables (e.g., GTT).

In order to estimate the necessary space for specific types of CCS translations, the STP should provide itemized “used” memory space information according to each CCS provisioning table. This granularity can provide enough information to estimate the amount of new CCS translations that can fit the available memory space by making various estimates according to “used” and “maximum” memory space.

Each supplier has limitations on certain systems engineering parameters related to CCS provisioning, so it is necessary that the proposal be a non-supplier-specific method of memory space accounting.

5.2.5.2 Methodology

To provide a supplier-independent method of memory space accounting, it is preferable to report on memory usage according to the user’s view of the STP provisioning tables. The most common user view that exists today is the view provided by the SEAS/STP Interface (GR-310-CORE and GR-778-CORE). This scheme would allow the user to inquire on a per-table basis the number of table entries in each table (defined below) that are still available to be populated. Therefore, the user will be able to determine, before entering a signaling order, if there will be enough room for all of the entries in a large recent change order. The number of entries available can be based on actual table data or on system parameters (e.g., the number of total signaling links that are available for an STP). If the STP cannot report table usage based on entries, then the STP shall use one of the methods outlined below.

R5-32 [332] The STP shall only report information about memory that is available to the user (i.e., unavailable “overhead” memory should not be included).

For each STP provisioning table listed below, the criteria for which combination of attributes uniquely identifies an entry is listed (see GR-310-CORE, Section 7.1 and GR-778-CORE, Section 3.1 for descriptions of the tables).

- Self Identity (SID)
  - Capability Code
- Link Set (LKS)
— LSSN or Far End Node PC/Far End Node ID

• Signaling Link (SLK)
  — LSSN/Member Number

• Destination (DST)
  — Destination PC

• Ordered Route (ORT)
  — Destination PC/LSSN

• Ordered Global Title Translation (GTT)
  — Translation Type/Global Title Range Begin/Global Title Range End/Destination PC/SSN

• Concerned Signaling Point (CSP)
  — Destination PC (Concerned Signaling Point)/PC/SSN

• Allowed Gateway Link Set (GLS)
  — LSSN

• Allowed Originating Point Code (OPC)
  — Screening Reference/Routing Label Originating Point Code

• Blocked Originating Point Code (BLKOPC)
  — Screening Reference/Routing Label Originating Point Code

• Allowed Service Information Octet (SIO)
  — Screening Reference/Network Indicator Code (NIC)/Service Indicator (SI)/Priority (PRI)/H0 Heading Code/H1 Heading Code

• Allowed Destination Point Code (DPC)
  — Screening Reference/Routing Label Destination Point Code

• Blocked Destination Point Code (BLKDPC)
  — Screening Reference/Routing Label Destination Point Code

• Allowed Affected Destination (DESTFLD)
  — Screening Reference/Affected Destination Point Code

• Allowed Calling Party Address (CGPA)
  — Screening Reference/Calling Party PC/SSN/Routing Indicator/Link Set Group Identifier
• Allowed Translation Types (TT)
  — Screening Reference/Translation Type

• Allowed Called Party Address (CDPA)
  — Screening Reference/Routing Label DPC/SSN/SCMG Format ID

• Allowed Affected PC/SSN (AFTPC)
  — Screening Reference/Affected PC/SSN.

If there is not a one-to-one mapping of the SEAS/STP type table entries (defined above) to the implementation of the translation tables, then the STP can provide an estimate.

However, it may be the case that some STP implementations may use a memory allocation scheme in which memory space is shared among several tables. In this case, it may not be possible to exactly specify how much memory is available for a particular table. In this case, the STP should report how much is available for a group of tables. For example, if a given number of gateway screening table entries are permitted, but there is no limit that any one table can use, then the STP can report that all of the gateway tables have a particular number of table entries remaining. The Memory Space Accounting Report will list all of the tables that can use this memory space.

If the STP cannot use any of the above methods, then the STP should provide a supplier-specific indication of how to calculate how much table space remains. For example, if a supplier cannot map their Global Title Translation Data to GTT table entries, they may supply information that will enable the user to calculate how much memory is available.

R5-33 [333] The STP shall support one or more of the following mechanisms (listed in decreasing order of preference) to report table usage:

... 1. The STP shall report the number of total and available entries (i.e., SEAS/STP entries) that the user can provision for each STP Basic and Gateway Provisioning Table listed below. In addition, the percentage of memory (i.e., the number of used entries as a percentage of total allocated space for that table) that is occupied in the table shall be able to be reported.

... 2. If the STP’s architecture prevents a one-to-one mapping of SEAS/STP table entries to the provisioning data as it is stored in the STP, then the STP has the option of providing an estimate (estimate will be of $\pm 10\%$ with 90% probability) of the number of table entries, available and total, percentage of memory occupied for that type of based on the average size entry in the particular translation table. The STP shall also indicate the percentage of memory occupied for that type of table. The STP shall indicate that this memory space accounting is an estimate.
3. If more than one table shares an allocation of memory and those tables are of a homogeneous nature (e.g., gateway screening tables), then the STP shall report the number of table entries available, maximum, and percent used as a group.

4. If more than one table shares an allocation of memory and those tables are not of a homogeneous nature and it is not possible to determine the number of entries used (e.g., based on system parameters such as the number of signaling links that are allowed) then the STP shall report the amount of memory total and available in bytes, the tables that use this memory, and the percent of memory available.

5. If it is infeasible or inaccurate for the STP to provide an accurate estimate of the number of total and available table entries, then the STP shall provide supplier-specific information related to the table via the supplier-specific parameter field in the Memory Space Accounting Report.

5.2.5.3 Reporting Requirements

R5-34 [334] The following SEAS/STP Interface Messages shall be provided to support the above:

- **On-demand Request for Memory Space Accounting** (SEAS to STP)
  Allows the user to request the amount of space that is being used in a particular table or tables. Message parameters will include the following:

  — Table(s) that memory space accounting is being requested for
  [The user shall be able to request that all tables be reported]

- **Memory Space Accounting Report** (STP to SEAS)
  Allows the STP to report the amount of memory that is available and the total amount of table memory, and the percentage of memory used in a table or tables. This message is the response to the Request for Memory Space Accounting. Message parameters will include

  — Table(s) for which memory usage is being reported
  — Number of entries available (unused) for table(s)
  — Number of total table entries allowed (allocated for)
  — Percentage of table space used
  — Estimate Indicator - indicates that the number of table entries available for this table is an estimate
… — Supplier-Specific Remarks - Allows the supplier to report any supplier-specific information about table usage that is specific to their implementation.

(Note: These messages will not be included in the forthcoming update of GR-310-CORE.)

Although the STP will be able to report memory usage on-demand, a mechanism will be needed to autonomously notify the user that the tables are becoming full.

R5-35 [335] The STP shall report table memory usage on-demand as well as when the percentage of table memory usage has crossed a user-defined threshold.

R5-36 [336] The user shall be able to specify three table memory usage thresholds on a per-table basis.

By being able to specify more than one threshold (e.g., defining thresholds of 50%, 75%, and 95%), the user can be alerted when the available space in a particular table is getting full. In addition, if the highest threshold is crossed, the report should have a priority of action of major. Otherwise, the priority of action should be minor. The use of multiple thresholds will alert the user continually as space is being used in the tables, allowing them to plan ahead for additional memory, but still letting them know when the tables are almost full.

R5-37 [337] The following SEAS/STP Interface Messages shall be provided to support the above:

… • Set Table Usage Threshold (SEAS to STP)
  Allows the user to set the thresholds at which the STP will send a report indicating that a memory usage threshold has been crossed. Message parameters will include

… — Table(s) for which the threshold is being set (or all tables)
… — Threshold 1 (0-99%)
… — Threshold 2 (0-99%)
… — Threshold 3 (0-99%).
… (Repeat for each table requested)

… • Query Table Usage Threshold (SEAS to STP)
  Allows the user to query the thresholds at which the STP will send a report indicating that a memory usage threshold has been crossed. Message parameters will include:

… — Table for which the threshold has been set (or all tables)
… — Threshold 1 (0-99%)
… — Threshold 2 (0-99%)
… — Threshold 3 (0-99%).
… (Repeat for each table requested)
… • Memory Space Accounting Threshold Crossing Report (STP to SEAS)
  Informs the user that a threshold has been crossed for memory usage for a given table. Message parameters will include
… — Priority of Action - Major (for highest threshold crossing), Minor (for other thresholds)
… — Table name - the name of the table for which this threshold has crossed.
… — Threshold crossed - the percentage level that was crossed
… — Number of entries available for table - the number of table entries that are still available for user population
… — Number of total table entries allowed - the maximum number of table entries that the user can populate.

(Note: These messages will not be included in the forthcoming update of GR-310-CORE.)

Figure 5-1. Entities
Figure 5-2. Relationship

Figure 5-3. Associative Entity
Figure 5-4. Composite Entity

Figure 5-5. Dependent Entity
Figure 5-6. Subtype Entity
Figure 5-7. Multi-Source Role Entity
Figure 5-8. MTP Routing Data Model
Figure 5-9. SCCP Routing Data Model
Figure 5-10. Generalization/Abstractions for Gateway Screening
Figure 5-11. Gateway Screening Data Model
6. STP Performance Management

6.1 Introduction

Performance management is the process of monitoring and controlling the operating condition of the STP and CCS network. Measurement data collected from the STP is used in various performance management functions. Traffic engineering functions use the data to size traffic sensitive STP resources and determine if additional signaling links are required. Similar measurement data, along with STP reported events, are used to detect equipment faults in real-time, and to determine if the network and STP meet service objectives over time. Performance management functions also use control capabilities to administer STP parameters, change the state of STP equipment, audit STP databases, and start or stop various STP functions. This section provides requirements to support the performance management functions listed above. The list below briefly describes the contents of each subsection that follows:

- **OS Interfaces (Section 6.2)** - This section provides background information about Operations Systems (OSs) that the STP must interface with.

- **Measured Entity Types (Section 6.3)** - This section describes the generic objects that are measured in the STP. Background information is provided in this section with no explicit requirements.

- **Measurement Requirements (Section 6.4)** - This section contains measurement requirements for the STP. Each subsection describes measurements required for a specific measured-entity type in the STP.

- **General Measurement Requirements (Section 6.4.1)** - This section provides general information on how to interpret the measurement requirements presented in subsequent sections, and provides requirements applicable to all measurements (e.g., requirements governing measurement accuracy, integrity, and security).

- **System Total Measurements (Section 6.4.2)** - This section contains requirements for measurements that monitor overall STP traffic, behavior, and performance.

- **Translation Type Measurements (Section 6.4.3)** - This section contains requirements for measurements that monitor traffic destined for a particular global title translation table.

- **Link Measurements (Section 6.4.4)** - This section contains requirements for measurements that monitor individual link traffic, behavior, and performance.

- **Processor Measurements (Section 6.4.5)** - This section contains requirements for measurements that monitor processor traffic and performance.

- **Link Set Measurements (Section 6.4.6)** - This section contains requirements for measurements that monitor link set behavior.
• **Measurement Reports (Section 6.5)** - This section describes requirements for reporting predefined groups of measurements to OSs.

• **Event reporting (Section 6.6)** - This section describes requirements for reporting significant STP detected events to an OS.

• **Control Capabilities (Section 6.7)** - This section describes requirements that support the administration of STP parameters and specific STP features of interest to operations personnel (e.g., such as special studies and the MTP Restart Procedure). This section also contains requirements for determining the state of STP equipment.

### 6.2 Operations System (OS) Interfaces

Operations Systems are used to collect measurement data and event reports from the STP. These OSs process and analyze the information to produce reports and drive alarm displays for Bcc personnel that monitor the CCS network. There are currently two OSs used to support the performance management functions. The SEAS™ System collects data from all STPs in the CCS network, providing an overall view of network performance. The SEAS System interfaces with the STP using the interface defined in GR-310-CORE, the SEAS/STP Interface Specification: User Program Layer (UPL) Application Message Descriptions and Functional Requirements. This interface specification describes the interactions used by the SEAS System to retrieve measurement data, collect event reports, and set STP administrative parameters. GR-310-CORE supports the collection of a large set of measurement data, some of which are not mentioned in the measurement requirements of the following sections. (GR-778-CORE provides additional requirements for the Gateway Screening Capability. This document also contains measurement requirements that must be met.) STP vendors are only required to provide the measurements listed in this document. Measurements appearing in GR-310-CORE that do not appear in this document are left as options, which the supplier may provide if they are applicable to their particular implementation. Many of the sections that follow will reference specific messages and terminology used in GR-310-CORE. In these cases, the text will explicitly show the relationship of the requirement to the GR-310-CORE specification.

The STP must also support an interface to a remote maintenance OS, which has responsibility for detecting specific equipment problems, including many that are not reported to the SEAS System. Messages sent to the remote maintenance OS may be supplier specific, indicating specific types of equipment failure. The format of these messages is not defined in this document. However, the interface used to send these messages to the remote maintenance OS is defined in TA-TSY-000387, *Generic Requirements for Interim Defined Central Office Interface (IDCI)*. STP capabilities necessary to support the remote maintenance function on transmission facilities are described in FR-475, *OTGR Section 5.0: Network Maintenance, Transport Surveillance*. Other capabilities supporting remote maintenance of the STP node are similar to those used
for switching systems, and are described in GR-474-CORE, *OTGR Section 4: Network Maintenance: Alarm and Control for Network Elements.*

Detailed requirements describing the interface to the SEAS System, the remote maintenance OS, and local craft work positions are in Section 8.

R6-1 [338] The STP shall provide the capabilities described in GR-474-CORE, and FR-475 to support the remote maintenance function.

To support the performance management functions, an OS other than the SEAS system may be used. As such, a generic interface for open system interconnection between NEs and OSs as described in GR-376-CORE, *OTGR Section 15.3: Generic Operations Interfaces Using OSI Tools: Network Data Collection (NDC),* may be used to support the transfer of traffic measurement data according to the full seven layers of the OSI protocol model. In addition, a set of generic interface messages used to convey network traffic management information between the STP and the Network Traffic Operations System (NTMOS) as described in GR-495-CORE, *Generic Operations Interfaces Using OSI Tools: Network Traffic Management,* may be used. GR-495-CORE provides generic message types for accomplishing the following functions: NE traffic monitoring, automatic and manual surveillance, automatic and manual controls, audits, and NE routing table alterations.

CR6-2 [339] As a per-Bcc option, the STP shall provide the capabilities described in GR-376-CORE and GR-495-CORE to support the performance management functions instead of providing the capabilities via the SEAS interface (as described in GR-310-CORE and GR-778-CORE) to support those functions. (Note, if this option is selected, it shall be understood that subsequent references to SEAS in the remainder of this section may not be applicable.)

6.3 Measured Entity Types

GR-310-CORE uses a hierarchical data collection request structure, where a measured entity type is defined as a class of objects from which measurement values are collected. (In this section, the term entity type refers to a measured entity type. It does not refer to the provisioning entity type described in Section 5.) Each object in that class generates the same set of measurements. This class of objects with similar measurement attributes is not limited to objects within the STP. For example, a link is defined as a measured entity type, since all instances of a link will have the same measurement attributes. An STP is also defined as a measured entity type, since all STPs exhibit similar behavior, in that they route MSUs and implement the network management procedures defined by SS7. Entity types could also be expanded to include STP features (e.g., ISNI and translation type mapping), although these entity types are not yet defined in GR-310-CORE. The entity types listed below are referenced in the following measurement requirements:
• Links
• Link sets
• Processors
• GTT translation tables
• Supplier specific equipment units
• Special studies.

Measurements are defined for each of these entity types in subsequent sections of this document. These requirements define the set of measurements the STP must maintain for each instance of an entity type. This generic model makes no assumptions as to the internal architecture of the STP (i.e., the way components are configured). Other entity types such as buffers, buffer groups (a collection of buffers sharing common memory), and processor groups (a collection of processors sharing load) may exist in a particular supplier implementation. Measurements on these entity types are allowed, and are explicitly supported by the GR-310-CORE interface if necessary for management of a particular implementation. Each of the required and optional entity types corresponds to one of the entity types defined in the GR-310-CORE interface specification.

6.4 Measurement Requirements

6.4.1 General Requirements

Each subsection below lists the measurements that must be maintained for each instance of an entity type. The measurement name is in bold letters, and corresponds directly to a measurement with the same name in the GR-310-CORE specification. [GR-310-CORE does not have a consolidated list of measurements with their associated definitions. The GR-310-CORE specification simply lists the measurements that are included in each report. The same measurement (maintained over different accumulation intervals) may be included in several reports. The measurement sections of this document provide a non-redundant list of measurements, providing a single definition for the measurement and all the accumulation intervals required.] Along with the measurement name, in parentheses, are the required accumulation intervals that the measurement values are maintained over. The following terms are used to describe the required accumulation intervals:

• 5 - every 5 minutes
• 30 - every 30 minutes
• h - every 60 minutes (hourly)
• d - every 24 hours (daily, with accumulation intervals ending at 12:00am)
m - marginal performance measurement. This measurement is kept on a 60 minute interval and thresholded. If a single marginal performance measurement crosses the assigned threshold, all measurements defined as a marginal performance measurements are reported to the remote maintenance OS in the signaling link marginal performance report.

Section 6.5 will describe how these measurements are grouped to form different reports sent over the GR-310-CORE interface and to a remote maintenance center. All measurements must meet the requirements described in GR-478-CORE, OTGR Section 8: Measurements and Data Generation for measurement accuracy, integrity, security.

Because this generic model is independent of implementation, the required measurements may not be sufficient to properly size internal STP resources. It will be necessary for the supplier to provide the proper measurements and methodology to size traffic sensitive internal STP resources.

**R6-3** [340] Each measurement in the following sections shall conform to the data quality requirements described in Sections 1.3 and 1.4 of GR-478-CORE.

The applicable requirements are found in the following sections of GR-478-CORE:

- 1.3.1 Measurement Accuracy
- 1.3.2 Measurement Integrity and Security.
- 1.4 Data Presentation.

**R6-4** [341] The supplier shall provide and document all measurements and methodology necessary to properly size traffic sensitive and feature sensitive STP resources (e.g., memory, processing, and bus capacity).

### 6.4.2 System Total Measurements

**R6-5** [342] The following measurements shall be maintained over the indicated accumulation intervals for the STP system:

... 1. **Originated Message Signal Units (5, 30)** - Number of outgoing MSUs, carrying the STP’s point code in the OPC field, that are successfully passed to MTP level 2 for transmission [e.g., network management messages and MSUs completing global title translation (GTT)].

... 2. **Terminated Message Signal Units (5, 30)** - Number of acknowledged, incoming MSUs carrying the STP’s point code or capability code in the DPC field.
3. **Through-Switched Message Signal Units (5, 30)** - Number of MSUs not carrying the STP’s point code or capability code in either the OPC or DPC. The MSU was acknowledged, translated, and successfully passed to MTP Level 2 for transmission.

4. **Originated MSU Octets (5, 30)** - Total number of octets associated with MSUs counted in the measurement “Originated Message Signal Units,” including those octets that will be added in MTP level 2 processing. The count must reflect the actual number of octets that will be transmitted.

5. **Terminated MSU Octets (5, 30)** - Total number of octets associated with MSUs counted in the measurement “Terminated Message Signal Units.” The count must reflect the actual number of octets received, including octets removed in MTP level 2 processing.

6. **Through-Switched MSU Octets (5, 30)** - Total number of octets associated with MSUs counted in the measurement “Through-Switched Message Signal Units,” including those octets that will be added in MTP level 2 processing. The count must reflect the actual number of octets that will be transmitted.

7. **Global Title Translations Performed (5, 30, d)** - Total number of MSUs successfully completing global title translation (i.e., a match was found for the global title). The count is kept across all translation types.

8. **Global Title Translations Unable to Perform: Translation Type Not Found (5, 30)** - Number of times the translation type specified in the MSU was not supported by the STP.

9. **Global Title Translations Unable to Perform: Incorrect Global Title Format (5, 30)** - Number of times the format of the global title was incorrect for the given translation type.

10. **Global Title Translations Unable to Perform: No Translation for This Address (5, 30)** - Number of times a match could not be found for the global title in the translation table. The count is kept across all translation types.

11. **Global Title Translations Unable to Perform: Incorrect GTA Data Reference (5, 30)** - Number of times the GTT process cannot be completed due to an incorrect GTA Reference, defined in Appendix J, Section J.1.

12. **Global Title Translations Unable to Perform: Incorrect Ordered DPC Reference (5, 30)** - Number of times the GTT process cannot be
completed due to an incorrect Ordered DPC Reference, defined in Appendix J, Section J.1.

... 13. **Global Title Translations Alternate Routed Due to Route Set Congestion** (5, 30) - Number of times, per congested point code and subsystem, that a message is alternate routed to the next preferred system when congestion is encountered for the route set to the indicated DPC.

... 14. **Duration of Node Internal Failure** (30) - Total time that messages could not be switched to an appropriate link for transmission, independent of link interface failures.

... 15. **Average Cross-STP Transport Time for Sampled MSUs** (30) - This count is made by sampling the cross STP transport time of an MSU every 10 seconds. The definition of cross STP transport time is described in Section 9. The sampled times are averaged by totaling the sampled times and dividing by the number of MSUs sampled over the measurement interval.

... 16. **Number of MSUs Sampled for Cross STP Transport Time** (30) - Number of MSUs sampled for cross STP transport time.

... 17. **Number of Sampled MSUs Failing Normal-Load 95th Percentile Test for Cross STP Transport Time** (30) - Number of MSUs sampled for cross STP transport time that did not meet the 95th percentile requirements specified for a Normal-Load STP in Section 9.

... 18. **Number of Critical System Alarms** (d) - The number of critical system alarms that occur over the measurement interval. The definition of a critical alarm is found in the section entitled Alarm Severity (Section 4.1.3.3) of TR-NWT-000474.

... 19. **Number of Major System Alarms** (d) - The number of major system alarms that occur over the measurement interval. The definition of a major alarm is found in the section entitled Alarm Severity (Section 4.1.3.3) of TR-NWT-000474.

... 20. **Number of Minor System Alarms** (d) - The number of minor system alarms that occur over the measurement interval. The definition of a minor alarm is found in the section entitled Alarm Severity (Section 4.1.3.3) of TR-NWT-000474.

... 21. **Number of Manual System Recovery Actions at/from Level nn** (d) - Number of manually initiated recovery actions at/from Level nn, where nn is an implementation defined recovery level (where nn is a number from 1 to 99).
22. **Total Time Spent in Manual System Recovery Actions at/from Level nn (d)** - Total time spent in manually initiated system recovery at/from Level nn, where nn is an implementation defined recovery level (from 1 to 99).

23. **Number of Automatic System Recovery Actions at/from Level nn (d)** - Number of automatically initiated recovery actions at/from Level nn, where nn is an implementation defined recovery level (from 1 to 99).

24. **Total Time Spent in Automatic System Recovery Actions at/from Level nn (d)** - Total time spent in automatic system recovery at/from Level nn, where nn is an implementation defined recovery level (from 1 to 99).

25. **Number of Audits (h, d)** - Number of audits initiated.

26. **Number Audits Encountering Irregularities (h, d)** - Number of audits that encounter irregularities.

27. **Number of Automatic Maintenance Interrupts (h, d)** - Number of automatically initiated maintenance interrupts. A maintenance interrupt is a system response to a trouble condition. Maintenance interrupts may perform service protection, localization, and fault isolation.

28. **Number of Manual Maintenance Interrupts (h, d)** - Number of manually initiated maintenance interrupts. A maintenance interrupt is a system response to a trouble condition. Maintenance interrupts may perform service protection, localization, and fault isolation.

29. **Equipment Unit Maintenance Usage (d)** - Total time that an equipment unit was manually made unavailable for use. This time is totaled across all equipment units of a particular type in the STP. This measurement is required for all equipment unit types in the STP implementation.

Note: An equipment unit is a field replaceable STP component that can be identified by STP diagnostics and fault isolation capabilities. Equipment unit types may include component types such as processors, memory boards, signaling terminals, etc. Since many equipment unit types will be supplier specific, equipment unit measurements (usage, faults, and errors) are specified as supplier specific measurements in the daily maintenance report (GR-310-CORE). However, some equipment unit types are generic and applicable to all implementations (e.g., processors), and have equipment unit measurements explicitly identified within their entity type. The required daily equipment unit measurements are totaled...
across all equipment units of a particular type. Because they are totaled counts (i.e., they are not measured for a specific instance of an equipment unit), they must be reported as supplier specific measurements under the entity type=STP in the daily maintenance report.

... 30. **Equipment Unit Errors (h, d)** - Number of troubles that cannot be verified under the processor’s program control. This count is summed across all equipment units of a specific type in the STP. This measurement is required for all equipment unit types in the STP implementation.

... 31. **Equipment Unit Faults (h, d)** - Number of troubles that can be verified under program control and lead to fault isolation. This count is summed across all equipment units of a specific type in the STP. This measurement is required for all equipment unit types in the STP implementation.

... 32. **Number of Equipment Units of Each Equipment Unit Type (30, h, d)** - Number of equipment units of each equipment unit type summed in the counts “Equipment Unit Maintenance Usage,” “Equipment Unit Errors,” and “Equipment Unit Faults.”

... 33. **MSUs Discarded Due to Invalid DPC (5, 30, h, d)** - Number of MSUs discarded because the STP cannot find the DPC in its translation table.

... 34. **MSUs Discarded Due to Invalid Service Information Octet (5, 30, h, d)** - Number of MSUs discarded because the STP does not support the service requested in the Service Information Octet.

... 35. **Average Node Processing Time for Sampled MSUs (30)** - This count is made by sampling the node processing time of an MSU every 10 seconds. The definition of node processing time is described in Section 9. The sampled times are averaged by totaling the sampled times and dividing by the number of MSUs sampled over the measurement interval.

... 36. **Number of MSUs Sampled for Node Processing Time (30)** - Number of MSUs sampled for node processing time.

... 37. **Number of Sampled MSUs Failing Normal-Load 95th percentile Test for Node Processing Time (30)** - Number of MSUs sampled for node processing time that did not meet the 95th percentile requirements specified for a Normal-Load STP in Section 9.
... 38. **Network Management Task Discard due to Queue Timeout (5)** - The number of network management tasks discarded because the task was queued for more than 1 minute by task priority.

... 39. **Number of MTP Restarts Initiated (h)** - Number of times MTP restart was initiated by the STP. This count does not include the number of times the MTP restart procedure was initiated as a result of messages from adjacent nodes.

... 40. **MSUs Discarded: Unrecognized SCCP Message Type (d)** - The number of MSUs discarded because the STP could not recognize an SCCP message type.

### 6.4.3 Translation Type Measurements

**R6-6** [343] The following measurements shall be maintained over the indicated accumulation intervals for each instance of a GTT table:

... 1. **GTT Performed (30)** - Total number of MSUs successfully completing global title translation (i.e., a match was found for the global title) for the particular translation type.

... 2. **GTT Error (no address found) (30)** - Number of times the “address not found” error was encountered for the particular translation type. (i.e., there was no match found for the global title in the GTT table)

... 3. **GTT Error (incorrect GTA Reference) (30)** - Number of times the “incorrect GTT data reference” error was encountered for the particular translation type or GTA because the GTA Reference could not be found, as described in Appendix J, Section J.1.

... 4. **GTT Error (incorrect Ordered DPC reference) (30)** - Number of times the “incorrect GTT data reference” error was encountered for the particular translation type or GTA because the Ordered DPC Reference could not be found, as described in Appendix J, Section J.1.

... 5. **GTTs Unable to Perform (30)** - Total number of global title translations unable to perform for the particular translation type (all reasons).

### 6.4.4 Link Measurements

**R6-7** [344] The following measurements shall be maintained over the indicated accumulation interval for each instance of a signaling link:
1. **MSUs Transmitted (30, d, m)** - Number of MSUs transmitted to the far end, including those MSUs that were retransmitted.

2. **MSUs Received (30, d, m)** - Number of MSUs received on the link, including those for which retransmission was requested.

3. **MSUs Retransmitted (m)** - Number of MSUs retransmitted by the near end.

4. **MSU Octets Transmitted (30, d)** - Number of octets associated with the MSUs counted in “MSUs Transmitted.” This count measures the total number of octets actually transmitted for all outgoing MSUs, including octets added in MTP level 2 processing.

5. **MSU Octets Received (30, d)** - Number of octets associated with the MSUs counted in “MSUs Received.” This count measures the total number of octets actually received for all incoming MSUs, before octets are removed in MTP level 2 processing.

6. **Link Maintenance Usage (30)** - The total time a link was manually made unavailable to MTP level 3 during the measurement interval.

7. **Duration of Link Outage (5, 30)** - Total time the link was unavailable to MTP level 3 during the measurement interval, regardless of whether the link was automatically or manually made unavailable.

8. **MSUs Received Requiring GTT (30)** - Number of incoming MSUs requiring GTT, regardless of the outcome of any gateway screening.

9. **MSU Octets Received for MSUs Requiring GTT (30)** - Total number of octets associated with the measurement “MSUs Received Requiring GTT,” including octets removed in MTP level 2 processing.

10. **Average Link Transmission Buffer Occupancy (octets) (30)** - This measurement requires that the transmit buffer occupancy (in octets) be sampled at regular scanning intervals. The measurement is made by summing the occupancy values obtained in each sample and dividing by the number of samples made.

11. **Total Duration of Level 1 Link Congestion (5, 30)** - Total time the link was in congestion Level 1 during the measurement interval. This total time is derived by summing the time duration of each individual level 1 link congestion event. A level 1 link congestion event begins when the level 1 congestion onset threshold is first reached or exceeded, or at the start of the measurement interval if the link is already at congestion level 1. The level 1 congestion event ends when one of the following occurs: i) the occupancy first falls below the level 1 congestion abatement threshold or ii) the occupancy reaches or
exceeds the congestion onset threshold for levels 2 or 3, or iii) the measurement interval ends.

12. **Duration of link congestion level 2 (5, 30)** - Total time the link was in congestion level 2 during the measurement interval. This total time is derived by summing the time duration of each individual level 2 link congestion event. A level 2 link congestion event begins when the level 2 congestion onset threshold is first reached or exceeded, or at the start of the measurement interval if the link is already at congestion level 2. The level 2 congestion event ends when one of the following occurs: i) the occupancy first falls below the level 2 congestion abatement threshold or ii) the occupancy reaches or exceeds the congestion onset threshold for level 3, or iii) the measurement interval ends.

13. **Duration of link congestion level 3 (5, 30)** - Total time the link was in congestion level 3 during the measurement interval. This total time is derived by summing the time duration of each individual level 3 link congestion event. A level 3 link congestion event begins when the level 3 congestion onset threshold is first reached or exceeded, or at the start of the measurement interval if the link is already at congestion level 3. The level 3 congestion event ends when one of the following occurs: i) the occupancy first falls below the level 3 congestion abatement threshold or ii) the measurement interval ends.

14. **Event Count for Entering Level 1 Link Congestion (5, 30)** - Number of times congestion level 1 was entered. Congestion level 1 is entered when the link was previously not congested, and the link transmission buffer occupancy at a given scan first reaches or exceeds the level 1 congestion onset threshold, but does not reach or exceed the congestion onset threshold for level 2 or 3.

15. **Event Count for Entering Level 2 Link Congestion (5, 30)** - Number of times congestion level 2 was entered. Congestion level 2 is entered when the link was previously not congested or at level 1, and the link transmission buffer occupancy at a given scan first reaches or exceeds the level 2 congestion onset threshold, but does not reach or exceed the congestion onset threshold for level 3.

16. **Event Count for Entering Level 3 Link Congestion (5, 30)** - Number of times congestion level 3 was entered. Congestion level 3 is entered when the link was previously not congested or at levels 1 or 2, and the link transmission buffer occupancy at a given scan first reaches or exceeds the level 3 congestion onset threshold.

17. **Priority 0 MSUs Discarded Due to Congestion (5, 30)** - Number of MSUs discarded due to congestion at levels 1, 2, or 3.
18. **Priority 1 MSUs Discarded Due to Congestion (5, 30)** - Number of MSUs discarded due to congestion at levels 2 or 3.

19. **Priority 2 MSUs Discarded Due to Congestion (5, 30)** - Number of MSUs discarded due to level 3 congestion.

20. **Priority 3 MSUs Discarded Due to Full Transmit Buffer (5, 30)** - Number of MSUs discarded due to a full transmit buffer.

21. **Average Link Output Delay for Sampled MSUs (30)** - This count requires that the link output delay of an MSU be sampled every 10 seconds, where the definition of link output delay is described in Section 9. The samples are totaled over the measurement interval and averaged by dividing by the number of MSUs sampled.

22. **Number of MSUs Sampled for Link Output Delay (30)** - Number of MSUs sampled for link output delay during the measurement interval.

23. **Link Active Time (d, m)** - Total time a link is in service and transmitting MSUs during the measurement interval.

24. **Link Available Time (d, m)** - Total time a link is available to MTP level 3.

25. **Number of Automatic Changeovers (d, m)** - Number of times the changeover procedure is used to move traffic from a link taken out of service to one or more alternate in-service links.

26. **Number of Hourly Thresholds Exceeded for Automatic Changeovers (d)** - An hourly threshold is used to determine if the previous measurement (Number of Automatic Changeovers) should appear on a signaling link marginal performance report for a particular hour. This measurement counts the number of times that threshold was exceeded (i.e., the number of signaling link marginal performance reports where that link was reported as having exceeded its threshold for automatic changeovers).

27. **Near End Forced Link Unavailable (d)** - Number of times a link was manually made unavailable to MTP level 3.

28. **Number of Far-end Management Inhibits (d)** - Number of times a link was successfully inhibited from the far end.

29. **Number of Signaling Link Declared Failures All Types (d)** - Number of times a signaling link has failed to prove in after an automatic changeover.
30. **Cumulative Duration of Signaling Link Declared Failures All Types (d)** - Total time that a signaling link is unavailable because of a declared signaling link failure.

31. **Cumulative Duration of Far-End Processor Outage (5)** - Total time that a link was unavailable to MTP level 3 due to the receipt of SIPO from the far end.

32. **Cumulative Duration of Busy-Link Status Units Received (5)** - Total elapsed time between the receipt of a Busy link status unit and the time when the next message is acknowledged, summed over all occurrences where a Busy link status unit was received.

33. **Number of Messages Signal Units Received in Error (d, m)** - Number of MSUs in which the MTP checksum indicated a transmission error.

34. **Number of Negative Acknowledgments Received (d, m)** - Number of times the Backward Indicator Bit was inverted, indicating the need to retransmit a group of MSUs.

### 6.4.5 Processor Measurements

R6-8 [345] The following measurements shall be maintained over the indicated accumulation intervals for each instance of a processor:

1. **Duration of Processor Outage (30)** - total time a processor is unable to perform one or more of its primary tasks. Primary tasks include, but are not limited to, those tasks that affect message processing, network management, or the ability to interact with external OSs.

2. **MSUs Processed Requiring GTT (30)** - If a processor is involved with MSU processing, this count must report the number of MSUs processed that required GTT.

3. **MSUs Processed Not Requiring GTT (30)** - If a processor is involved with MSU processing, this count must report the number of MSUs processed that do not require GTT.

4. **Real-time Available to Process Additional Messages (30)** - Number of milliseconds available for processing additional messages during the measurement interval.

5. **Real-time Spent in Overhead Functions (30)** - Number of milliseconds used by the processor to perform overhead functions.
6. **Real-time Spent in MTP Functions (MSU Processing) (30)** - Number of milliseconds used by the processor to perform MTP functions related to MSU processing.

7. **Real-time Spent in MTP Functions (Network Management) (30)** - Number of milliseconds used by the processor to perform MTP functions related to network management.

8. **Real-time Spent in SCCP Functions (MSU Processing) (30)** - Number of milliseconds used by the processor to perform SCCP functions related to MSU processing.

9. **Real-time Spent in SCCP Functions (Network Management) (30)** - Number of milliseconds used by the processor to perform SCCP functions related to network management.

10. **Processor Utilization (30)** - Total time the processor was busy, divided by the total time in the measurement interval.

11. **Message Discard from Signaling Message Handling Overload (5)** - A count of all messages, by priority, that are discarded due to a signaling message handling processor overload condition.

12. **Signaling Message Handling Overload Duration (5)** - A per-overload level (if the multiple overload level option is used) duration that a processor performing signaling message handling functions is in processor overload.

13. **Signaling Message Handling Overload Event Count (5)** - A per-overload level (if the multiple overload level option is used) count of the number of times that a given signaling message handling processor overload level is reached.

[346] It is an objective that the following measurements should be maintained over the indicated accumulation intervals for each instance of a processor:

1. **Processor Maintenance Usage (h)** - Total time that a processor is manually made unavailable for use.

2. **Processor Errors (h)** - Number of processor troubles that cannot be verified under program control.

3. **Processor Faults (h)** - Number of troubles detected in a processor that can be verified under program control and lead to fault isolation.
6.4.6 Link Set Measurements

R6-10 [347] The STP shall provide the following measurements on a per-link-set basis:

— **Traffic Diversion to Lower Priority Link Set (30, h)** - This measurement applies to STPs with E-links to signaling endpoints on a remote cluster. In this scenario, the E-links are the highest priority route to those signaling endpoints in the remote cluster, with the B-links between the STP pairs as a lower priority route. This measurement counts the number of times traffic was diverted from the higher priority E-links to the lower priority B-links.

— **Duration of Diverted Traffic (30, h)** - This measurement is the duration (in seconds) that traffic is diverted from higher priority E-links to lower priority B-links, for STPs that have E-links to signaling endpoints on a remote cluster.

— **MSUs Transmitted (30)** - Number of MSUs transmitted to the far end, including those MSUs that were retransmitted.

— **MSUs Received (30)** - Number of MSUs received on the link, including those for which retransmission was requested.

— **MSU Octets Transmitted (30)** - Number of octets associated with the MSUs counted in “MSUs Transmitted.” This count measures the total number of octets actually transmitted for all outgoing MSUs, including octets added in MTP level 2 processing.

— **MSU Octets Received (30)** - Number of octets associated with the MSUs counted in “MSUs Received.” This count measures the total number of octets actually received for all incoming MSUs, before octets are removed in MTP level 2 processing.

— **MSUs Received Requiring GTT (30)** - Number of incoming MSUs requiring GTT, regardless of the outcome of any gateway screening.

— **MSU Octets Received for MSUs Requiring GTT (30)** - Total number of octets associated with the measurement “MSUs Received Requiring GTT,” including octets removed in MTP level 2 processing.

— **Total Duration of Link Set Inactivity (30)** - Total time that all links in the link set were unavailable to MTP level 3 during the measurement interval, regardless of whether the links were automatically or manually made unavailable.
6.4.7 Special Study Measurements

CR6-11 [348] The following measurements should be maintained over the indicated accumulation intervals for each instance of a special study, as a per Bcc option:

1. MSUs Received with Specified OPC/DPC/SIO on a Link Set (30) - Number of incoming MSUs acknowledged on the specified link set with the specified OPC/DPC/SIO combination.

2. MSU Octets Received With Specified OPC/DPC/SIO on a Link set (30) - Number of octets associated with the measurement “MSUs received with specified OPC/DPC/SIO on a Link set,” including those octets that will be added in MTP level 2 processing. The count must reflect the actual number of octets that will be transmitted.

3. MSUs Transmitted With Specified OPC/DPC/SIO on a Link Set (30) - Number of outgoing MSUs successfully transmitted to the far end on the specified link set with the specified OPC/DPC/SIO combination.

4. MSU Octets Transmitted with Specified OPC/DPC/SIO on a Link Set (30) - Number of octets associated with the measurement “MSUs Transmitted With Specified OPC/DPC/SIO on a Link Set,” including those octets that will be added in MTP level 2 processing. The count must reflect the actual number of octets that will be transmitted.

6.4.8 Equipment Unit Type

O6-12 [349] It is an objective that the following measurements be maintained over the indicated accumulation intervals for each instance of an implementation specific equipment unit:

1. Equipment Unit Maintenance Usage (d) - Total time that an equipment unit was manually made unavailable for use. The time is provided for each instance of an equipment unit of a particular type, and is provided for all equipment unit types in the STP.

Note: An equipment unit is a field replaceable STP component that can be identified by STP diagnostics and fault isolation capabilities. Equipment unit types may include component types such as processors, memory boards, signaling terminals, etc. Since many equipment unit types will be supplier specific, equipment unit measurements (usage, faults, and errors) are specified as supplier specific measurements in the hourly maintenance report (GR-310-CORE).
2. **Equipment Unit Errors (d)** - Number of troubles that cannot be verified under program control. This count is provided for each instance of an equipment unit of a particular type, and is provided for all equipment unit types in the STP.

3. **Equipment Unit Faults (d)** - Number of troubles detected that can be verified under program control and lead to fault isolation. This count is provided for each instance of an equipment unit of a particular type, and is provided for all equipment unit types in the STP.

### 6.5 Measurement Reports

At the end of each accumulation interval, measurements are grouped into predefined reports that are sent to the SEAS System, the remote maintenance OS, or local work positions. Measurement reports sent to the SEAS System must comply with the data collection requirements documented in the GR-310-CORE. The SEAS System supports several data collection methods that include scheduled polling, scheduled autonomous reporting, and on-demand polling by the STP. Messages used to support the data collection process are defined in the section entitled Data Collection Messages (Section 6) of GR-310-CORE. Appendix B of GR-310-CORE lists the predefined reports supported by the SEAS System-SP interface, the data collection method used to retrieve the report, and the measurements contained in the report. Some predefined reports in GR-310-CORE include measurements that are not explicitly listed as required in this document. The collection of these measurements is left as a vendor option, if they are applicable for a particular implementation. The STP is only required to provide those measurements listed as required in Section 6.4 of this document. Other reports may be delivered to a remote maintenance OS using the interface stated in TA-TSY-000387. The requirements below indicate the measurement reports that must be supported by the STP, and provide references to other requirements documents for the format and interface used to transmit the report to a destination OS.

**R6-13** [350] All measurement reports sent to the SEAS System shall conform to the response time requirements defined in the section entitled STP Response Times to the SEAS System Commands (Section 11.3.2) and in the section entitled Response Times for Autonomous Messages (Section 11.3.3) of GR-310-CORE.

### 6.5.1 STP System Total Report

The STP System Total Report contains measurements of the total traffic processed by the STP over a half hour interval. The specific measurements included in this report are found in GR-310-CORE, Appendix B.
R6-14 [351] The STP shall provide the STP System Total Report to the SEAS System, as described in Appendix B of GR-310-CORE.

6.5.2 Component Measurement Report

The STP Component Measurement Report contains measurements of component utilization used primarily for traffic engineering. The specific measurements included in this report are found in GR-310-CORE, Appendix B.

R6-15 [352] The STP shall provide the Component Measurement Report to the SEAS System, as described in Appendix B of GR-310-CORE.

6.5.3 Service Measurement Report

The STP Service Measurement Report contains measurements of STP real time performance, measuring the processing delays encountered by sampled MSUs. The specific measurements included in this report are found in GR-310-CORE, Appendix B.

R6-16 [353] The STP shall provide the Service Measurements Report to the SEAS System, as described in Appendix B of GR-310-CORE.

6.5.4 Special Study Report

The STP Special Study Report contains the results of any special studies that may be active in the STP. The specific measurements included in this report are found in GR-310-CORE, Appendix B.

CR6-17 [354] As a per-Bcc option, the STP should provide the Special Study Measurements Report to the SEAS System, as described in Appendix B of GR-310-CORE.

6.5.5 Daily Maintenance Measurement Report (SEAS System)

The Daily Maintenance Report contains measurements that help detect STP and network problems. The Daily Maintenance Measurement Report sent to SEAS must include the measurements defined for it in GR-310-CORE, Appendix B.

R6-18 [355] The STP shall provide the Daily Maintenance Report to the SEAS System, as described in Appendix B of GR-310-CORE.
6.5.6 Daily Maintenance Report (Remote Maintenance OS & Local Craft Terminal)

The Daily Maintenance Report must also be available to the remote maintenance OS and local craft terminal.

R6-19 [356] The STP shall provide a Daily Maintenance Report to the remote maintenance OS and local craft terminal that includes all the daily measurements identified in Section 6.4.

R6-20 [357] The STP shall support scheduling the output of the Daily Maintenance Report to the remote maintenance OS and local craft terminal for any time up to 24 hours after the end of the accumulation interval.

R6-21 [358] The STP shall not allow the Daily Maintenance Report to be inhibited.

R6-22 [359] The STP shall supply the Daily Maintenance Report on an on-demand basis to the remote maintenance OS and local craft terminal any time up to 24 hours after the end of the accumulation interval.

6.5.7 Day to Hour Maintenance Measurement Report (SEAS System)

Maintenance measurements are normally reported every 24 hours. It may be necessary for Bcc personnel to obtain the current value of maintenance measurements accumulating during the day. The STP must support requests for the on-demand day to hour maintenance report from SEAS. The measurements included in the on-demand day to hour maintenance report for SEAS are described in GR-310-CORE, Appendix B.

R6-23 [360] The STP shall provide the on-demand Day to Hour Maintenance Report to the SEAS System, as described in Appendix B of GR-310-CORE.

6.5.8 Day to Hour Maintenance Report (Remote Maintenance OS & Local Craft Terminal)

The STP must also provide the Day to Hour Maintenance Report to the remote maintenance OS and local craft terminals.

R6-24 [361] The STP shall provide the on-demand Day to Hour Maintenance Report to the remote maintenance OS and local craft terminal. This report
shall include the current values of all the accumulating daily measurements identified in Section 6.4.


6.5.9 Signaling Link Marginal Performance Report

Several link measurements may provide an early indication of link problems. These link measurements are thresholded at the STP, and are only reported to the remote maintenance OS if thresholds are crossed. The signaling link marginal performance report is described in GR-478-CORE, Section 6, and should be sent to the remote maintenance center over the TA-TSY-000387 (IDCI) interface. This report should also be reported to the local craft terminal.

R6-27 [364] The STP shall support the administration of marginal performance thresholds for link measurements defined as being marginal performance measures in Section 6.4.

R6-28 [365] The STP shall send the signaling link marginal performance report as described in Section 6 of GR-478-CORE to the remote maintenance OS.

6.5.10 Hourly Maintenance Report (SEAS System)

The Hourly Maintenance report permits maintenance personnel more frequent access to significant overall system performance measurements. The measurements contained in the Hourly Maintenance Report sent to SEAS are described in GR-310-CORE, Appendix B.

R6-29 [366] The STP shall provide the Hourly Maintenance Report to the SEAS System, as described in Appendix B of GR-310-CORE.

6.5.11 Hourly Maintenance Report (Remote Maintenance OS & Local Craft Terminal)

The Hourly Maintenance Report must also be sent to the remote maintenance OS and local craft terminal.
The STP shall also send the Hourly Maintenance Report to the remote maintenance OS. This report shall include all the hourly measurements identified in Section 6.4.

6.5.12 Autonomous Network Management Reports & 5 Minute Exception Reporting

Many of the same counts used for engineering and maintenance are also of use in monitoring network traffic flows in near real time. The Autonomous Network Management Report described in Appendix B of GR-310-CORE provides Bcc personnel with access to many of these counts on a 5-minute interval. This permits faster detection and resolution of developing network problems. To reduce the amount of data normally transmitted to the SEAS System, the link measurements defined in this report are excluded, unless there are non-zero measurements for the link. All link measurements in the Autonomous Network Management Report that are non-zero should be included in the report, in the section for ENTTYPE=LINK.

The STP shall send a subset of the Autonomous Network Management Report to the SEAS System, as described in Appendix B of GR-310-CORE. The subset consists of all the measurements required by this document that are listed in the section ENTTYPE=STP of the Autonomous Network Management Report.

The link measurements defined in the Autonomous Network Management Report shall be excluded, unless there are non-zero measurements for the link. All non-zero link measurements shall be reported in the section of the Autonomous Network Management Report for ENTTYPE=LINK.

6.6 Event Reporting

This section provides requirements for reporting significant STP detected events to the following destinations:

- A remote maintenance OS, using TA-TSY-000387
- The SEAS System system, using the interface specified in GR-310-CORE.

Significant events include internal equipment problems detected by the STP, or the receipt of certain SS7 messages indicating network troubles. Events that indicate problems affecting more than one STP (i.e., network troubles) are reported to both the SEAS System and the remote maintenance OS. Expected network troubles that must be reported are enumerated in the requirements of Section 6.6.2. Events that indicate internal STP
problems (e.g., non traffic affecting STP outages) are only reported to the remote maintenance OS and local craft terminals. These events will likely be specific to a particular implementation, and are not enumerated in this document at this point in time. All event reports must be reported in real-time. Event reports made to the SEAS System provide an indication of the initial failure in a REPT message, followed by an indication that the STP has recovered from the failure in a RCVRY message. \(^1\) It is important that all failure and recovery notifications occur in pairs (except where explicitly noted), and in the proper sequence. For example, if a link should fail, the failure notification must be sent over the SEAS System channel before the recovery notification. As described below, each notification must also be time stamped to show the actual order and time at which the events occurred in the STP.

There are other event types used to trace problems that are provided only when maintenance personnel are studying a particular problem. Reports of these types of troubles are provided as part of a trap capability, described in Section 6.6.3.

### 6.6.1 Event Report Content

**R6-33** [370] All event reports sent to the remote maintenance OS and the local craft interface (those associated with the trap capability, those reporting real-time network troubles and STP internal problems) shall include the general information described below.

- Event ID - The specific trouble reported by the network or detected by the STP.
- Time Stamp - The time the event was detected. The time shall be reported to the nearest second.
- Component ID - The common language code (or other identifier) for the signaling link or other equipment that received the message or on which the trouble was detected.
- Sequence Number - A unique, ordered number associated with each network trouble event used at a network center to determine when messages from a particular STP are missing.

**R6-34** [371] All internal STP equipment problems shall be reported to the remote maintenance OS and local craft terminals.

**R6-35** [372] The event types listed in Section 6.6.2 shall be reported to the remote maintenance OS and local craft terminals.

---

1. The REPT and RCVRY messages are defined in Section 8 of GR-310-CORE.
[R6-36] The event types listed in Section 6.6.2 shall be reported to the SEAS System over the GR-310-CORE interface, and must follow the associated message syntax and format defined in the section entitled On-Occurrence Autonomous Messages (Section 8) of GR-310-CORE. Note: Each event type listed in Section 6.6.2 identifies the corresponding GR-310-CORE On-Occurrence Autonomous Message.

[R6-37] All event reports sent to the SEAS System shall conform to the response time requirements defined in the section entitled Response Times for Autonomous Messages (Section 11.3.3) in GR-310-CORE.

[R6-38] The REPT message for a GR-310-CORE event type shall be reported before the accompanying RCVRY message for that event.

### 6.6.2 Event Report Types

[R6-39] The following event types shall be reported to the remote maintenance OS, local craft terminals, and to the SEAS System:

- Inability to Perform a Global Title Translation (REPT-NOTRNS) - This event indicates the STP received an MSU requiring GTT and encountered a problem identified in the list below. The event shall indicate which of the following problems was encountered.
  - Requested Translation Type does not exist
  - Global title could not be found in the translation table
  - Invalid format for global title field.
  - GTA Reference could not be found (see Appendix J, Section J.1)
  - Ordered DPC Reference could not be found (see Appendix J, Section J.1).

Note: GR-310-CORE specifies screening features to reduce the quantity of translation errors reported to the SEAS System.

- MTP Translation Error (REPT-MTPERR) - This event is reported when an incoming MSU requiring translation encounters one of the following problems:
  - DPC does not match the STP’s self identity (i.e., its point code or any of its capability codes), and DPC does not have a route specified for it in the Ordered Route entity set of the STP’s provisioning tables.
— MSU’s Service Information Octet (SIO) indicates an invalid Service Indicator (i.e., an invalid user of the MTP) or an invalid Network Indicator Code.

Note: GR-310-CORE specifies screening features to reduce the quantity of translation errors reported to the SEAS System.

- Link Congestion Level Increase (REPT-LINK-CGST) - This event indicates that a transmit congestion onset or discard threshold has been reached with buffer occupancy in the increasing direction. The event report shall identify the level of overload and congestion threshold that was reached (i.e., onset or discard).

- Recovery from Link Congestion (RCVRY-LINK-CGST) - This event indicates that a transmit congestion abatement threshold has been crossed with buffer occupancy in the decreasing direction. The message shall be sent as the congestion abatement threshold for each congestion level is reached.

- Near-End Manually Made Link Unavailable (REPT-LNK-MANUAV) - This event indicates that a link was manually made unavailable to MTP level 3. The event shall indicate whether the link was manually inhibited or manually deactivated.

Note: this message is listed as for further study in GR-310-CORE. This may replace the previous message REPT-LNK-MGTINH.

- Near-End Manually Made Link Available (RCVRY-LNK-MANUAV) - This event indicates that a link was manually made available to MTP level 3. The event shall indicate whether the link was manually uninhibited or manually activated.

Note: this message is listed as for further study in GR-310-CORE. This may replace the previous message REPT-LNK-MGTUNH.

- Link Failure (REPT-LKF) - This event indicates that a link available to MTP level 3, was automatically made unavailable to MTP level 3 for reasons outlined in Chapter T1.111.3 and T1.111.4 of GR-246-CORE (e.g., excessive errors, excessive delay, etc.). This event notification shall indicate the reason for the link failure. If the restoral of the link will be delayed due to the link oscillation filter (see Section 4.2.10), then this event notification shall include an indication of the delay and the amount of the delay (i.e., the remainder of T1.111.4/T32 or T1.111.4/T34) in the report.

- Recovery from Link Failure (RCVRY-LKF) - This event indicates that a failed link, as defined in the Link Failure message, has been made available to MTP level 3.
• Link Set Outage (REPT-LKSTO) - This event indicates that all links in a link set are unavailable to MTP Level 3 routing.

• Recovery from Link Set Outage (RCVRY-LKSTO) - This event indicates that at least one link in a previously unavailable link set is now available to MTP Level 3 routing.

• Far-End Processor Outage (REPT-PRO) - This event indicates that SIPO is being received from the far-end terminal and the far-end processor is out of service. Note: SIPO must be received for longer than T1.111.4/T1, before this event report is generated.

• Far-End Processor Recovered (RCVRY-PRO) - This event indicates the far-end terminal has stopped sending SIPO, and the far-end has recovered from processor outage.

• No Route to Adjacent Node (REPT-RTEUAV) - This event indicates the route set to an adjacent node has become unavailable.

• Route Available to Adjacent Node (RCVRY-RTEUAV) - This event indicates that a route set to an adjacent node, which was previously unavailable, is now available to MTP level 3.

• Commencement of MTP Restart Procedures (REPT-MTP-RSTRT) - This event indicates the STP has initiated the MTP restart procedures. This event does not include the initiation of MTP restart as a result of messages from an adjacent node.

• Progress of MTP Restart (REPT-STATUS-RSTRT) - This event provides information every 30 seconds about the status of an active MTP restart procedure at the STP. As an option, the supplier may include the percentage and number of links available in the status message. This event does not include the progress of MTP restart initiated as a result of messages from an adjacent node. Note: This message provides only progress information.

• Completion of MTP Restart Procedures (RCVRY-MTP-RSTRT) - This event indicates the STP has completed the MTP Restart Procedure. This event does not include completion of MTP restart initiated as a result of messages from an adjacent node.

• Start of Lower Priority Route (REPT-LOW-RTE) - This event applies when an STP begins to utilize a lower priority route other than the C-link set to route traffic toward a given destination address, because the higher priority route specified for that destination has become unavailable. A separate message shall be generated for each lower priority route (destination-link set pair) that is receiving such alternate-routed traffic.
Return to Higher Priority Route (RCVRY-LOW-RTE) - This event indicates that routing has been restored over the higher priority route to a signaling point on a remote cluster, and that routing for that point is no longer being made over the lower priority (non C-link) route. A separate message shall be generated for each lower priority route (destination-link set pair) that was, but is no longer, receiving such alternate-routed traffic.

Administrative Processor Congestion or Overload (REPT-ADMPR-CGST) - This event indicates the onset of STP administrative processor congestion or overload. The definition of congestion or overload for the administrative processor is implementation specific. These messages should be generated only when a communications session with the SEAS System is active, and should not be buffered at the STP.

Recovery from Administrative Processor Congestion or Overload (RCVRY-ADMPR-CGST) - This event indicates recovery from STP administrative processor congestion or overload.

Message Handling Processor Overload (REPT-MHPRC-OVLD) - This event indicates when a processor overload condition is encountered for a processor performing message handling functions.

Message Handling Processor Overload Level Change (REPT-MHPRC-OVLC) - This event indicates when a processor overload level changes (increases or decreases, if the multiple overload level option is used, or when the overload is no longer present).

Isolated Message Handling Processor Capacity Reduction (REPT-MHPRC-ISLCR) - This event indicates that the STP has initiated or stopped sending TFRs via the response method for a capacity reduction of the resource(s) associated with message handling that is unlikely to exist at its mate and is causing a danger of congestion. The notification shall include an identification of the problem that is causing the capacity reduction.

Isolated Message Handling Processor Capacity Recovery (RECVRY-MHPRC-ISLCR) - This event indicates that the STP has stopped sending TFRs via the response method for a previous capacity reduction of the resource(s) associated with message handling that was unlikely to exist at its mate and was causing a danger of congestion. The notification shall include an identification of the event resulting in the recovery from the problem that was causing the capacity reduction.

Network Management Task Priority Discard Threshold Reached (REPT-NMTSK-DSCD) - This event indicates when a threshold of an
internal priority buffer is reached at which task discarding may take place.

- Recovery From Network Management Task Priority Discard Processing (RECVY-NMTSK-DSCD) - This event reports that the STP’s processor(s) handling MTP and/or SCCP network management functions have recovered from an overload condition such that the STP is no longer discarding buffered lower priority network management tasks.

- Unexpected MTP Network Management Message Received (REPT-UNXP-MTPNM) - This event indicates that the STP received a network management message it did not expect. The event message shall identify the point code sending the unexpected message and shall indicate which of the following occurred:
  - Unexpected TFR received - This event occurs when an STP that performs cluster routing for the affected point code receives a TFR for that point code, and the cluster is prohibited on the affected route.
  - Unexpected TFA received - This event occurs when an STP that performs cluster routing for the affected point code receives a TFA for that point code, and the cluster is not allowed via the affected route.

- Removal of member from x-list due to timeout (REPT-XLST-TIMO) - This event indicates that an error condition is suspected because the status of a member on the x-list did not change before the corresponding timer (i.e., Tx-list timer) expired and no traffic destined to the member was routed through the STP while the timer was running.

- Unrecognized SCCP Message Type (REPT-UNRC-SCCPMT) - This event notification is reported when the STP receives an unrecognized SCCP message type. (The message is discarded in this case.)

- MTP Loop Detected: Prohibited Destination (REPT-MTPLP-DET) - This event indicates that a circular route was detected because the STP received a circular route test message that it initiated. The event report should contain the affected destination, the route that was tested and its cost, the route the test message was received on, and the trigger used to detect the loop (i.e., one of: congestion trigger, provisioned routing change, routing status change).

- Sustained Prohibited Destination Due to Detected MTP Loop (REPT-MTPLP-SUST) - This event indicates that a destination is still prohibited due to the detection of an MTP circular route (i.e., the STP
received a circular route test message that it initiated). The event report should contain the affected destination, the original detection time, the cost of the route the loop was detected on, and the number of reminders given for this destination. This reminder shall be given every 30 minutes after the detection of the loop, until maintenance changes the status of the destination to allowed.

... • Resumption of Traffic to Destination Previously Prohibited Due to MTP Loop Detection (RCVRY-MTPLP-RST) - This event indicates that maintenance cleared the “prohibited due to MTP loop detection” status for the affected destination. The event report should contain the affected destination.

... • Priority 3 MSU Discard - This event is reported when the STP discards a priority 3 message. To reduce the potential number of reports, only the first detected discarded message after the fourth signaling message handling congestion discard threshold is reached should be reported. If the monitored congestion falls below the third signaling message handling congestion abatement threshold and then reaches the fourth signaling message handling congestion discard threshold again, the first detected discarded message should be reported.

... Note: a corresponding SEAS System message has not yet been defined.

... • SCCP Hop Counter Violation (REPT-SCCP-HOPCTV) - This event notification is reported when the SCCP Hop Counter is equal to zero due to the STP decrementing the SCCP hop counter for a given message.

CR6-40 [377] Initiation of the STP network management priority processing shall be reported, when the priority processing capability is initiated based on the processor overload, as a per Bcc option.

6.6.3 Trapping Capabilities

Trapping capabilities provide information in near real-time about SS7 messages that would not normally be kept by the system. The objective of these capabilities is to provide CCS network maintenance personnel with information to assist in detecting and resolving CCS network failures. In general, trapping capabilities refer to those functions that examine and compare certain SS7 message fields in each SS7 message processed by a CCS node against a set of specified message trapping data (i.e., criteria); the contents of those SS7 messages having SS7 message fields that match the specified trapping criteria are then reported.
6.6.4 Routing Verification Tests

As discussed in Section 4.4, the STP must support the MTP Routing Verification Test (MRVT) and SCCP Routing Verification Test (SRVT) defined in OMAP. These tests are useful for detecting errors in MTP routing and global title translation tables respectively.

6.7 Control Capabilities

6.7.1 Administration of Network Management Parameters

Many of the SS7 procedures use timer values to determine when specific actions must take place. GR-246-CORE provides recommended ranges for timer values. Table 6-1 at the end of this section shows either the minimum settable range or accuracy range and a provisional value for timers described in GR-246-CORE. When a minimum settable range is specified, the timer must be provisionable; the accuracy of the timer should then be +/-10% of the provisioned value except when indicated otherwise for T1.111.4/T19. When an accuracy range is specified, the timer need not be provisionable, but its value should be within the specified range.

R6-42 [379] In addition to automatic network management controls described in T1.111.3 and T1.111.4 of GR-246-CORE, the STP shall also provide controls necessary to support automatic initiation of network management processing priority described in Section 4.2.4.

R6-43 [380] Supplier-provided documentation shall provide the default values for all adjustable parameters, including protocol timers and transmission buffer congestion thresholds. The document shall provide any constraints that may exist on changing these parameters (such as maximum and minimum values).

R6-44 [381] If parameter adjustments become necessary, the STP supplier shall provide the reason for the adjustments and a mechanism to implement the adjustments.

R6-45 [382] Buffer congestion thresholds shall be adjustable on a per-link set basis. 2
R6-46 [383] Unless indicated otherwise, timer values specified in Table 6-1 shall be adjustable on a per node basis.

R6-47 [384] The STP shall provide the current values of network management parameters when requested to do so, using the In-Service Record Base Measurements Message described in Appendix B of GR-310-CORE.

CR6-48 [385] MTP Level 2 timers (timers T1-T7 of T1.111.3 in GR-246-CORE) shall be adjustable on a per-link-set basis, if the STP is interfaced to the networks of exchange or interexchange carriers that use links which are not 56 kbps terrestrial links (e.g., satellite or lower bit rate).

O6-49 [386] It is an objective that the STP should support the adjustment of timers and buffer congestion thresholds through the control messages detailed in section entitled Application Control Messages (Section 9) of GR-310-CORE.

R6-50 [387] The STP shall provide the capability to administer parameters (i.e., processor thresholds, timers, priority assignments) used for network management priority processing.

CR6-51 [388] As a per-Bcc option, network management processor occupancy thresholds that are used for priority processing of network management tasks shall be adjustable on a per-processor basis, as the optimum setting will depend on the processor capacity and its architecture.

6.7.2 Administration of Special Studies

Special studies are measurement reports that determine traffic flows between two nodes in the CCS network. These studies allow users to count MSUs routed from an OPC (or set of OPCs) to a DPC (or set of DPCs). The specific Service Information Octet specified in the MSU can also be included as a special study parameter. The results of a special study are reported to the SEAS System in a predefined report documented in Appendix B of GR-310-CORE. Requirements for reporting special study results are found in Section 6.5. CR6-52 [389] and CR6-53 [390] describe an objective for how special study parameters should be administered.

CR6-52 [389] As a per Bcc option, the STP shall support the administration and collection of measurements for up to 100 simultaneously running special studies.

---

2. Optimum settings will depend on the engineered load and mixture of traffic of different priorities that use the link set.
CR6-53 [390] As a per-Bcc option, the STP should support the administration of special studies parameters through the control messages described in the section entitled Application Control Messages (Section 9) in GR-310-CORE.

6.7.3 Retrieval of Maintenance Status

During regular operations activity, it may be necessary for maintenance personnel to obtain the maintenance state of a specific piece of STP equipment. The STP must be capable of supplying the remote maintenance OS and the SEAS System with the maintenance state of STP equipment.

R6-54 [391] The STP shall send the maintenance state of STP equipment to the SEAS System using the Maintenance Status Report, as described in Appendix B of GR-310-CORE.

R6-55 [392] The STP shall support sending the maintenance state of STP equipment to the remote maintenance OS.

6.7.4 Signaling Link Maintenance

A signaling link has three major components: a transmission link and two signaling link terminals. The signaling link terminals are any hardware and software within the CCS signaling node required to provide the physical and link layers of the MTP in the SS7 protocol. The transmission link is the facility and network terminal equipment connecting the two signaling link terminals. The signaling link maintenance process generally follows the path described in GR-474-CORE, Section 4.2.6. R6-56 [393] through R6-58 [395] and O6-59 [396] are in addition to those in GR-474-CORE, Section 4.2.6.

R6-56 [393] Signaling link tests are described in T1.111.7 of GR-246-CORE. The STP shall support these tests as stated in the requirements in Section 4.2.5 of this document.

R6-57 [394] The local control and display interface shall be capable of displaying the basic maintenance state (e.g., active, out-of-service, or unavailable) of each link and link set in the STP.

R6-58 [395] The local control and display information shall also be made available to the remote maintenance OS.
O6-59 [396] It is desirable that the STP provide Signaling Data Link Test capabilities as described in T1.111.7 of GR-246-CORE for performing loopback tests on 56-kb/s links.

6.7.5 Capabilities to Support MTP Restart

The MTP restart procedure allows an unavailable STP to bring a sufficient number of signaling links into the available state, and to update its routing tables before telling adjacent nodes that it is able to carry user signaling traffic. This procedure is described in Section 4.2.4.7 of this document. R6-60 [397] and R6-61 [398] describe the maintenance capabilities necessary to support the node restart capability. Section 6.6.2 describes event reporting requirements related to the MTP restart procedure.

R6-60 [397] The STP shall delay any administrative or maintenance functions that may have detrimental affects on the MTP restart procedure.

To support MTP restart, the provisioning of a control parameter that allows CCS network personnel to either enable or disable the MTP restart procedures on a per STP-basis should be provided by the STP, as described by the mtp_restart_indicator attribute of the STP entity, in Section 5.2.3.5.

R6-61 [398] allows CCS network personnel to modify the default value of the MTP restart control parameter, as Section 5.2.3.5 describes. The MTP restart procedures may be automatically invoked if the control parameter is set to ‘enable’. If the control parameter is set to ‘disable’, MTP restart procedures may not be automatically invoked. Initially, the MTP restart procedures will have a default value of ‘enable’.

R6-61 [398] If MTP restart procedures are invoked and CCS network personnel modify the MTP restart control parameter from ‘enable’ to ‘disable’, the modified control parameter shall be effective upon completion of the currently invoked MTP restart procedures and the node shall notify CCS network personnel that MTP restart procedures are currently in progress and the parameter change will take effect after completion.
Table 6-1. Ranges and Provisional Values for Timers

Range refers to the minimum settable range except when the value is marked with “*,” in which case it refers to the accuracy range. Provisional Values refer to the current Bellcore recommended default values.

<table>
<thead>
<tr>
<th>MTP Level 2 Timers</th>
<th>Description</th>
<th>Provisional Value</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1.111.3 Timer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Timer for aligned and ready condition</td>
<td>13 sec.</td>
<td>12.9-16 sec. *</td>
</tr>
<tr>
<td>T2</td>
<td>Timer for out-of-alignment status</td>
<td>11.5 sec.</td>
<td>5-14 sec. *</td>
</tr>
<tr>
<td>T3</td>
<td>Timer for aligned condition</td>
<td>11.5 sec.</td>
<td>5-14 sec. *</td>
</tr>
<tr>
<td>T4n</td>
<td>Normal proving period</td>
<td></td>
<td>+/- 10% accuracy</td>
</tr>
<tr>
<td></td>
<td>— for 56-kbps signaling links</td>
<td>2.3 sec.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— for 64-kbps signaling links</td>
<td>2.0 sec.</td>
<td></td>
</tr>
<tr>
<td>T4e</td>
<td>Emergency proving period</td>
<td></td>
<td>+/- 10% accuracy</td>
</tr>
<tr>
<td></td>
<td>— for 56-kbps signaling links</td>
<td>0.6 sec.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— for 64-kbps signaling links</td>
<td>0.5 sec.</td>
<td></td>
</tr>
<tr>
<td>T5</td>
<td>Busy status transmission interval</td>
<td>100 msec.</td>
<td>80-120 msec. *</td>
</tr>
<tr>
<td>T6</td>
<td>Supervision of remote congestion timer</td>
<td>3 sec.</td>
<td>1-6 sec.</td>
</tr>
<tr>
<td>T7</td>
<td>Excessive delay of acknowledgment</td>
<td>0.5 sec.</td>
<td>0.5-2 sec.</td>
</tr>
</tbody>
</table>

* - refers to accuracy range rather than minimal settable range
### Table 6-1. Ranges and Provisional Values for Timers (Continued)

#### MTP Level 3 Timers

<table>
<thead>
<tr>
<th>Timer</th>
<th>Description</th>
<th>Provisional Value</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>Transmission delay following changeover</td>
<td>0.5 sec.</td>
<td>500-1200 ms.</td>
</tr>
<tr>
<td>T2</td>
<td>Changeover acknowledgment timer</td>
<td>0.7 sec.</td>
<td>0.7-2 sec.</td>
</tr>
<tr>
<td>T3</td>
<td>Transmission delay following changeback</td>
<td>0.5 sec.</td>
<td>500-1200 ms.</td>
</tr>
<tr>
<td>T4</td>
<td>Changeback acknowledgment timer (first attempt)</td>
<td>0.5 sec.</td>
<td>500-1200 ms.</td>
</tr>
<tr>
<td>T5</td>
<td>Changeback acknowledgment timer (subsequent attempt)</td>
<td>0.5 sec.</td>
<td>500-1200 ms.</td>
</tr>
<tr>
<td>T6</td>
<td>Controlled rerouting transmission delay</td>
<td>0.5 sec.</td>
<td>500-1200 ms.</td>
</tr>
<tr>
<td>T7</td>
<td>Waiting for signaling data link connection acknowledgment</td>
<td>1.5 sec.</td>
<td>1-2 sec.</td>
</tr>
<tr>
<td>T8</td>
<td>Transfer-prohibited inhibited timer (transient solution)</td>
<td>1 sec.</td>
<td>800-1200 ms.</td>
</tr>
<tr>
<td>T9</td>
<td>not used</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T10</td>
<td>Signaling-route-set-test message transmission interval</td>
<td>30 sec.</td>
<td>30-60 sec.</td>
</tr>
<tr>
<td>T11</td>
<td>Transfer-restricted timer</td>
<td>90 sec.</td>
<td>30 to 90 sec.</td>
</tr>
<tr>
<td>T12</td>
<td>Uninhibit acknowledgment timer</td>
<td>1 sec.</td>
<td>800-1500 ms.</td>
</tr>
<tr>
<td>T13</td>
<td>Forced uninhibit acknowledgment timer</td>
<td>1 sec.</td>
<td>800-1500 ms.</td>
</tr>
<tr>
<td>T14</td>
<td>Inhibit acknowledgment timer</td>
<td>3 sec.</td>
<td>2-3 sec.</td>
</tr>
<tr>
<td>T15</td>
<td>Signaling-route-set-congestion-test interval</td>
<td>3 sec.</td>
<td>2-3 sec.</td>
</tr>
<tr>
<td>T16</td>
<td>Transfer-controlled update timer</td>
<td>1.4 sec.</td>
<td>1.4-2 sec.</td>
</tr>
</tbody>
</table>
### Table 6-1. Ranges and Provisional Values for Timers (Continued)

<table>
<thead>
<tr>
<th>Timer</th>
<th>Description</th>
<th>Provisional Value</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>T17</td>
<td>Timing to restart of initial alignment</td>
<td>1 sec.</td>
<td>800-1500 ms.</td>
</tr>
<tr>
<td>T18</td>
<td>Waiting to repeat TFR once by the response method</td>
<td>under study</td>
<td>2-20 sec.</td>
</tr>
<tr>
<td>T19</td>
<td>Timeout for attempting link activation</td>
<td>8 min.</td>
<td>8-10 min. ‡</td>
</tr>
<tr>
<td>T20</td>
<td>Waiting to repeat local inhibit test</td>
<td>120 sec.</td>
<td>90 to 120 sec.</td>
</tr>
<tr>
<td>T21</td>
<td>Waiting to repeat remote inhibit test</td>
<td>120 sec.</td>
<td>90 to 120 sec.</td>
</tr>
<tr>
<td>T22</td>
<td>Timer at restarting SP waiting for signaling links to become available</td>
<td>60 sec</td>
<td>36-60 sec. †</td>
</tr>
<tr>
<td>T23</td>
<td>Timer at restarting SP, started after T22, waiting to receive all traffic restart allowed messages</td>
<td>60 sec</td>
<td>9-60 sec. †</td>
</tr>
<tr>
<td>T24</td>
<td>Timer at restarting SP with transfer function, started after T23, waiting to broadcast all traffic restart allowed messages</td>
<td>60 sec</td>
<td>9-60 sec. †</td>
</tr>
<tr>
<td>T25</td>
<td>Timer at adjacent SP and restarting SP, waiting for traffic restart allowed message - may be started at Level 3</td>
<td>under study</td>
<td>30-35 sec.</td>
</tr>
<tr>
<td>T26</td>
<td>Timer at restarting SP waiting to repeat traffic restart waiting message</td>
<td>under study</td>
<td>12-15 sec.</td>
</tr>
<tr>
<td>T27</td>
<td>Minimum duration of unavailability for full restart</td>
<td>under study</td>
<td>2-5 sec.</td>
</tr>
</tbody>
</table>

† - denotes a range not stated in GR-246-CORE
‡ - required accuracy is -0%,+25%
### Table 6-1. Ranges and Provisional Values for Timers (Continued)

#### MTP Level 3 Timers

<table>
<thead>
<tr>
<th>Timer</th>
<th>Description</th>
<th>Provisional Value</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>T28</td>
<td>Timer at SP adjacent to restarting SP waiting for traffic restart waiting message</td>
<td>under study</td>
<td>4-6 sec.*</td>
</tr>
<tr>
<td>T29</td>
<td>Timer started when TRA sent in response to unexpected TRA or TRW; also started when traffic resumed without receipt of TRA</td>
<td>under study</td>
<td>60-65 sec.</td>
</tr>
<tr>
<td>T30</td>
<td>Timer to limit sending of TFPs and TFRs in response to unexpected TRA or TRW</td>
<td>under study</td>
<td>30-35 sec.</td>
</tr>
<tr>
<td>T31</td>
<td>False link congestion detection timer</td>
<td>30 sec.</td>
<td>10-120 sec.</td>
</tr>
<tr>
<td>T32</td>
<td>Link oscillation timer - Procedure A</td>
<td>60 sec.</td>
<td>60-120 sec.</td>
</tr>
<tr>
<td>T33</td>
<td>Probation timer for link oscillation - Procedure B</td>
<td>60 sec.</td>
<td>60-600 sec.</td>
</tr>
<tr>
<td>T34</td>
<td>Suspension timer for link oscillation - Procedure B</td>
<td>60 sec.</td>
<td>5-120 sec.</td>
</tr>
<tr>
<td>T_{brdcst}</td>
<td>Timer to limit the time sending broadcast method TFP/TCP messages</td>
<td>7 sec.</td>
<td>0-15 sec.</td>
</tr>
</tbody>
</table>

* - denotes a narrower range than in GR-246-CORE

#### Signaling Link Test Timers

<table>
<thead>
<tr>
<th>Timer</th>
<th>Description</th>
<th>Provisional Value</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>Supervision timer for signaling link test acknowledgment message</td>
<td>4 sec.</td>
<td>4-12 sec.</td>
</tr>
<tr>
<td>T2</td>
<td>test messages</td>
<td>90 sec.</td>
<td>30-90 sec.</td>
</tr>
<tr>
<td>T_{loop}</td>
<td>Supervision timer for circular route test</td>
<td>10 sec.</td>
<td>10-20 sec.</td>
</tr>
</tbody>
</table>

---

6–37
Table 6-1. Ranges and Provisional Values for Timers (Continued)

### SCCP Management Timer

<table>
<thead>
<tr>
<th>Timer</th>
<th>Description</th>
<th>Provisional Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>T(status info.)</td>
<td>Delay for subsystem-status test</td>
<td>30 sec.</td>
</tr>
</tbody>
</table>
7. Network Management

This section has been consolidated into Section 6.
8. System Interfaces

R8-1 [399] The STP shall support interfaces for the signaling links, for communications with OSs, and for work stations used by operations personnel.

8.1 Signaling Interfaces

Section 3.1 gives an overview of the SS7 protocol. Section 4 specifies SS7 capabilities required for STP signaling. This section addresses the physical level interface requirements.

At the physical level, CCS links are defined as signaling data links. They are bidirectional transmission paths (i.e., two channels operating together in opposite directions at the same data rate).

R8-2 [400] Transmission facilities shall be digital.

R8-3 [401] The data rate of the channel shall be 56 kb/s except for possibly gateway STPs as discussed in Appendix C.

R8-4 [402] The signaling data link shall be exclusively dedicated to CCS use between two SPs.

R8-5 [403] At least one of the following types of physical level interfaces shall be provided:

... • The interface to a Data Service Unit/Channel Service Unit (DSU/CSU) in the CO. The required interface to connect the signaling terminal equipment to a transmission link is specified in CCITT Recommendation V.35, CCITT Working Party XI/2.

... • A 4-wire interface that carries the DS0A signal between the STP and a Digital Data Service (DDS) terminal equipment within a Central Office (CO). The signal is a bipolar non-return-to-zero format with the nominal 64-kb/s DS0 signal clocking derived from the composite clock signal. Refer to TA-TSY-000077, Digital Channel Banks—Requirements for Dataport Channel Unit Functions.

While the DS0 interface is the most desirable, in certain situations the CCITT Recommendation V.35 interface may be required.

Signaling link trouble detection capabilities shall be provided, as Section 6.2 specifies.
8.1.1  Synchronization Requirements for DS0A Interfaces

R8-6  [404] When DS0A interfaces are utilized, external Composite Clock (CC) references shall be required.

The composite clock signal is described in Section 5.1 of GR-378-CORE, Generic Requirements for Timing Signal Generators. The DS0A signal requirements are described in TR-TSY-000458, Digital Signal Zero A (DS0A) Systems Interconnection, and its timing requirements are described in GR-1244-CORE, Clocks for the Synchronized Network: Common Generic Criteria. The need for bit and byte synchronization on the DS0A signal makes CC the only acceptable timing reference; DS1 timing references are not acceptable for DS0A signals.

8.1.1.1  CC Redundancy Requirements

R8-7  [405] Both primary and secondary CC references shall be used.

R8-8  [406] The STP shall provide means to automatically detect a Loss-Of-Signal (LOS) on its active reference at its timing interface and select the alternate reference, which might be 180 degrees out of phase. Also, due to cabling lengths, there might be a time delay between the two reference signals of up to 2.7 microseconds, which shall be accommodated.

R8-9  [407] Switching between references shall cause no more than one errored signal unit for any DS0A link. This applies to both automatic switching due to CC LOS and manual switching initiated by craft or OS interface.

8.1.1.2  CC Robustness Requirements

The STP is required to be robust to redundant CC reference failures. Redundant CC reference failures are uncommon, but do occur. This section contains requirements for maximum recovery time of physical layer data so that the higher layers of the SS7 protocol may restore the link to service as quickly as possible. There are two types of impairments that may occur on redundant CC reference signals, phase hits and LOS.

8.1.1.2.1  CC Phase Hits

Phase hits are defined to be changes in the phase of the signal that are instantaneous or rapid. A rapid change in phase can be translated to an average fractional frequency change by dividing the magnitude of the phase step by the time duration of the phase step.
R8-10 [408] The STP shall follow phase hits on the CC reference signal.

R8-11 [409] GR-378-CORE allows for phase hits on the CC reference signal up to 1 microsecond in magnitude with a rate of change of 81 nanoseconds in 1.326 milliseconds (representing an average fractional frequency offset of 61 ppm (parts per million)). No data errors shall occur for these phase hits.

R8-12 [410] For phase hits that have magnitudes larger than 1 microsecond or represent average frequency changes larger than 61 ppm, or are instantaneous, physical layer, errors may occur on the DS0A physical layer data. After the phase hit has ended, the STP shall begin transmitting physical layer DS0A data that is phase aligned with the CC reference within 250 milliseconds of the time when the phase hit has ended.

R8-13 [411] The STP shall tolerate phase flips on the CC reference signal, which might generate an improper bipolar violation in the CC signal. This impairment shall cause no more than one errored signal unit on any DS0A link.

8.1.1.2.2 CC LOS

DS0A data transmission is not possible without the presence of the CC signal. If the STP experiences a LOS on both CC signals and holdover is not provided, it is recognized that DS0A data traffic will be lost. When the CC signal is restored it is important that the data be restored as quickly as possible.

R8-14 [412] After a LOS on both CC references, the STP shall begin transmitting physical layer DS0A data that is phase aligned with the CC reference, which may have an arbitrary phase relationship with respect to the phase before the LOS event, within one second of the time when either the primary or secondary CC signal is present.

Because of the critical need for phase alignment for DS0A signals, long-term (on the order of hours) holdover is not considered feasible. This is because the source (the Building Integrated Timing Supply [BITS]) for the phase alignment at the other end of the DS0A link may also experience phase drift due to both normal wander or a fault condition of its own. Some holdover capability may add robustness to the system. It is recognized that failures due to impairments on the synchronizing signal may also cause failures at the other end of the associated intraoffice DS0A data link. These features will not protect against failures at far end equipment. They are included because it is also recognized that there are failure modes that, while infrequent, can cause loss of synchronization to specific equipment and may affect only the STP end of a data link. This SS7 signaling equipment is sufficiently
important that some companies may want the extra service protection afforded by these optional features.

**CR8-15** [413] The STP may be required to bridge outages of both primary and secondary CC references by providing holdover.

Requirements **R8-16 [414]**, **R8-17 [415]**, **CR8-18 [416]**, **R8-19 [417]**, **R8-20 [418]**, and **R8-21 [419]** apply if holdover is provided.

**R8-16** [414] During the first 15 seconds of holdover, there shall be less than 500 nanoseconds of phase movement on the internal CC signal as measured at the transmitted DS0A signal.

**R8-17** [415] Entry into holdover shall cause no more than 1 signal unit error.

**CR8-18** [416] Longer holdover periods may be required.

**R8-19** [417] As the phase drift of the DS0A data increases, eventually the DS0A data will be far enough misaligned from the office CC that data errors will occur. When the signal unit error rate monitor exceeds its threshold the link shall be taken out of service and no attempt shall be made to restore until the external CC reference is restored.

**R8-20** [418] If the CC signal is restored within the period where the DS0A data is still phase aligned (the link is not experiencing errors), recovery from holdover shall cause no more than 1 signal unit error.

**R8-21** [419] If the CC signal is restored past the period where the DS0A data is no longer phase aligned (the link is experiencing errors), restoration of the physical layer DS0A data that is phase aligned to the external CC signal shall occur within one second.

### 8.2 OS Interfaces

The Bccs are using many OSs to provide centralized support for maintenance and administration of switching systems. Most companies provide an Operations Systems Network (OSN) for the data communications needs of some of these interfaces.

A standard operating environment for OS data communications is BX.25, which is based on CCITT Recommendation X.25. The design goals of BX.25 were to specify procedures to be used between Data Terminal Equipment (DTE) communicating directly, and to allow a BX.25 DTE to communicate through an X.25-based OSN. The BX.25 protocol specification, PUB 54001, is publicly available. TR-TSY-000510, *LSSGR: System Interfaces*, describes the BX.25 protocol and compares it with CCITT Recommendation.
X.25. Bellcore operates the BX.25 Interactive Test Facility, which provides specific information about an implementation’s degree of conformity to the BX.25 specification.

For CCS network operations support system interfaces, either dedicated facilities or an OSN may be used with the BX.25 protocol. The physical level may use the RS-232-C interface or the higher speed CCITT V.35 or RS-449 interfaces.

An interface specification document is available for each interface, stating specific requirements for options, parameters, and the required subset of protocol capabilities at each level.

8.2.1 STP/SEAS System

The SEAS system data communication interface to the STP may be point-to-point or via an OSN. Details of the interface are provided in the STP/SEAS System Interface Specification in GR-310-CORE.

The interface enables the STP to send traffic, routing, and performance data to the SEAS system on a scheduled basis and on demand. Additionally, a subset of maintenance measurements and the trouble event reports and network management reports are sent to the SEAS system on a scheduled basis and on occurrence for network surveillance functions. The data and reports sent to SEAS are described in Section 6 of this document. Through the SEAS system, administrators can enable and disable collection of measurement data in the STP by measurement set, by component, or by specific measurement.

8.2.2 STP Remote Maintenance System

Section 6 describes remote maintenance capabilities.

R8-22 [420] The interface between the remote maintenance operation system and the STP shall conform to one of the following, as specified by the Bcc:

… 1. The interface to the No. 2 Switching Control Center System (No. 2 SCCS) shall be provided via the asynchronous or synchronous interface as described in TA-TSY-000387.

… 2. The standard communication protocol and language as described in GR-828-CORE and in TR-TSY-000827, Generic Operations Interfaces Non-OSI Communications Architecture. FR-439 describes the functional interface standards that identify the logical application modules on both sides of the interface. The standard command response messages that carry operation information across the interface are defined in GR-833-CORE.
8.3 Operations Work Positions

The STP shall support interfaces for on-site and remote work positions necessary to support the provisioning and maintenance functions of the STP. Section 6.5 contains more detailed requirements for maintenance. Section 5.1 defines provisioning and administration capabilities.

R8-23 [421] The STP shall provide three types of work position interfaces: an on-site Input/Output (I/O) work position, a remote I/O work position, and a control and display interface.

8.3.1 I/O Work Positions

R8-24 [422] Alphanumeric devices such as teletypewriters or Cathode Ray Tube (CRT)-keyboard terminals shall be provided with the STP for operating, administering, and maintaining the system.

R8-25 [423] A printer shall also be provided that produces a copy of the input and output messages sent to the maintenance channel.

R8-26 [424] All I/O work position devices shall be able to communicate with the STP to which they are connected, independently and simultaneously, without disrupting service at the STP.

R8-27 [425] If trouble is detected in the communication between the STP and the device, so that the device is automatically taken out of service, the craftsperson previously active at the device shall be able to reestablish the interaction on an operative device in less than 30 minutes. This capability is required to allow critical functions to be performed.

R8-28 [426] Thus, a craftsperson shall be able to determine the results of the commands before the interruption.

8.3.1.1 On-Site I/O Work Positions

O8-29 [427] It is desirable that a single I/O device provide all required on-site operations functions if the following criteria can be met:

… • Provisioning I/O does not mask maintenance alarm messages

… • The device can be switched to maintenance functions at any time to provide emergency operations.
R8-30  [428] If these criteria cannot be met, separate devices shall be provided for maintenance functions and provisioning functions. (Maintenance functions are discussed in Section 6.1.7 and provisioning functions are discussed in Section 5.2.)

R8-31  [429] The option for separate terminals for each on-site function shall be provided.

8.3.1.2 Remote I/O Work Positions

R8-32  [430] The STP shall provide interfaces for remote STP work stations in Bcc centralized work centers. Section 6.5 describes remote maintenance requirements.

O8-33  [431] A remote work position for provisioning and administration capabilities should be an option.

R8-34  [432] The remote work position shall feature an RS-232-C interface, and support a dedicated line to the remote site or a permanent access via an OSN.

8.3.1.3 I/O Characteristics

R8-35  [433] It is required that input commands, output messages, and a character set conform to the user system interface and user system language standards (including syntax, semantics, and acknowledgments) as stated in TR-TSY-000825, *OTGR: User System Interface - User System Language*.

R8-36  [434] All I/O commands shall be categorized by operational function for message routing, echoing, and security purposes.

R8-37  [435] Each I/O command shall be allotted to one or more categories by a system administrator through the use of the command facility.

8.3.1.4 Message Routing and Echoing

R8-38  [436] It shall be possible to specify which output command categories are to be directed to which device by operator command.

R8-39  [437] Maintenance commands entered through the STP on-site work position shall be echoed to the remote maintenance work position. Input
commands entered through the remote work position shall be echoed to the STP on-site maintenance work position.

R8-40  
**[438]** The entry of memory administration commands or related commands at on-site or remote work positions that change provisioning data or related operational parameters at the STP shall result in corresponding notifications being sent to the SEAS system. These include any modifications of STP routing translations, SS7 link and port assignments, SS7 Gateway message screening tables, SS7 protocol parameters (e.g., timers and link congestion thresholds), and any other provisioning data elements described in Section 5.2.

R8-41  
**[439]** For these notifications sent to the SEAS system, the STP shall use appropriate autonomous message formats described in GR-310-CORE.

R8-42  
**[440]** Notifications for commands resulting in changes to data administered via SEAS system RC&V commands shall be formatted as an “STP Recent Change Interrupt” autonomous message as defined in Section 8.1 of GR-310-CORE.

R8-43  
**[441]** Notifications for commands resulting in changes to other memory administration data, including any supplier-specific provisioning commands, shall be formatted as an “STP Flow-Through Autonomous Message” as defined in Section 10.3 of GR-310-CORE.

O8-44  
**[442]** It is desirable that the SEAS system commands resulting in these changes be printed or displayed at the STP and at the remote maintenance center and/or be logged in the STP.

### 8.3.2 STP Control and Display Interface

R8-45  
**[443]** A control and display interface, such as a CRT device, shall be provided for manual control capability, and display of service and maintenance status of the overall system as well as the major equipment subsystems.

R8-46  
**[444]** If the control and display device is combined with the I/O device, the following criteria shall be met:

...  
- The status display of major system components shall not be masked by I/O functions.

...  
- Control and display functions can be obtained at any time despite system sanity.
8.4 Security of Operations Interfaces

R8-47 [445] The STP shall conform to Bellcore requirements for network element security in GR-815-CORE.
9. Performance

9.1 Reliability

The STP downtime objectives are directly related to the CCS network unavailability objective, which corresponds to an average of no more than 10 minutes cumulative downtime per year between two Signaling End-Points, and applies only to the Message Transfer Part of the SS7 protocol. This objective has been recommended by CCITT, proposed by Bellcore, and adopted by ANSI (Committee T1). Figure 9-1 shows downtime allocation for different segments of the CCS network.

9.1.1 General Considerations

A link interface provides signaling link access to an STP, and failure modes associated with the link interface affect only the link(s) terminating on it. Link interface unavailability is the probability that the link interface is not available for signaling traffic. This interface unavailability is included in an STP Signaling Link’s (in short, STP Link) unavailability. Links having common or equivalent destinations should terminate on different link interfaces. Failure modes associated with the STP processor(s) are assumed to be independent of the link interface failure modes.

R9-1 [446] STPs shall be designed to operate in a mated pair configuration.

The STP downtime objectives stated below are for a single STP operating in a mated pair configuration. Any other deployment of an STP (not one of a mated pair) in a CCS network requires demonstration that the CCS network unavailability objective stated above is met.

STP downtime may be caused by hardware or software failures, procedural errors, or other factors. To model hardware reliability, it is not always practical to specify the hardware downtime requirement as a fixed portion of the downtime attributed to failures from all causes. To address this, a new set of reliability requirements for downtime have been proposed in Supplement 1 of GR-512-CORE, to be used directly and unambiguously for hardware reliability modeling only. Thus, in accordance to GR-512-CORE, LSSGR: Reliability Section 12 and its Supplement, STP reliability is defined in terms of “Service (all causes) Downtime Objectives” and “Hardware Downtime Requirements” for the CCS network nodes.

9.1.2 Service (All Causes) Downtime Objectives

These downtime objectives are intended to control the amount of time that STPs are unavailable to provide service due to failures from all causes (hardware, software, procedural errors, and other factors). Downtime caused by normal Operations,
Administration, & Maintenance (OA&M) activities is counted against the service (all causes) downtime objectives. The reason for including the OA&M activities is their potential degrading effect on system reliability, which depends on their implementation and the architecture of the system.

Service (all causes) downtime objectives were usually stated as a single number equal to the unavailability, or average population downtime during some specified period, typically one year. However, these objectives are the averages of probability distributions. Because the STP downtime objectives are small compared to the average restoration time, it is expected that a large percentage of STPs will experience zero downtime during a year while others will experience downtime greater than the objectives. These performance characteristics are important Bcc service considerations not directly addressed by an average downtime objective.

Performance and reliability objectives are best stated by statistical statements about the average of the expected performance, and the distribution characteristics. To better reflect end-user service expectations and to control excessive downtime, statements of STP downtime objectives should include conditions that over a specified time period, it is expected that no more than a given percentage of STPs have downtime exceeding a specific value.

When stating or referring to downtime objectives for STPs it should be clear to what level of the SS7 protocol they apply. STPs relay messages from one signaling node to another at the MTP level 3, and also provide processing functions at higher levels, such as SCCP. Current Bellcore requirements for STPs do not require ISDN-UP processing because ISDN-UP messages in the STP are MTP-routed. Also, TCAP functions are applicable to STPs that have OMAP capability.

When referring to downtime objectives for services using STPs it should be understood if the SCCP level of the STP is used. For example, in the 800 Service one STP may do Global Title Translation (GTT), thus using the SCCP function in addition to the MTP function, while another STP may use only MTP functions. As discussed later, there are separate STP downtime objectives for the MTP and SCCP.

9.1.2.1 MTP Level

The two downtime objectives stated below apply only to the Message Transfer Part of the SS7 protocol.

---

1. GR-512-CORE, LSSGR: Reliability, Section 12, gives a list of these OA&M activities that includes: preventive maintenance, hardware fault repair, software patching, office data change, diagnostics, generic update, program backup, and data backup.

2. The STPs currently in Bcc signaling networks do not have OMAP functions and thus, TCAP functions are not yet applicable to STPs. However, a combined SSP/STP node may contain both TCAP and ISDN-UP functions but these are considered to be SSP functions.
9.1.2.1.1  **STP Total System Downtime**

STP Total System Downtime refers to a state in which the STP loses all CCS capability.

O9-2 [447] It is an objective that the average Total System Downtime of an STP population be less than 3 minutes per year in any year of operation, and no more than 1% of the STPs in the population be down for more than 110 minutes per year from all causes (including hardware, software, and procedural errors).

The STP Total System Downtime per year is a cumulative downtime calculated for each STP. The STP Total System Downtime was called “STP common” in previous issues of this document.

9.1.2.1.2  **STP Link Downtime**

STP Link Downtime refers to a state in which an individual link (e.g., A-, B-/D-, C-, or E-link) is out of service because of failures in the STP.

O9-3 [448] It is an objective that the average Link Downtime of an STP link population be less than 85 minutes per year for each year of STP operation, and no more than 5% of the STP links in the population be down for more than 8.5 hours per year from all causes (including hardware, software, and procedural errors).

The STP Link Downtime per year is a cumulative downtime calculated for each STP link. The STP Link Downtime is different from the “STP Link-Specific Downtime” used in previous issues of this document. STP Link Downtime is calculated as the sum of downtime predictions from all causes (including hardware, software, and procedural errors) for each of the failure modes that cause an outage of one or more STP Links (including those failure modes that cause a total loss of CCS capability for the STP). The STP Link Downtime includes what was called “STP common” and “STP Link-Specific” downtime.

It is important to recognize that the “STP Link Downtime” does not include downtime of the link transport facility. R9-4 [449] considers the time within which an STP should start link alignment after a transport facility recovers.

R9-4 [449] When a transport facility is restored after a failure, it shall take not more than 30 seconds for the STP to start link alignment, except for the following cases:

3. When the probability of zero-downtime during a year is greater than 0.95, a 5% point cannot be defined. In these cases, 1% points will be specified. Otherwise, 5% points will be specified.
... • When the link is deliberately not being restored due to the link oscillation filter or due to a prioritized link restoral after a massive link failure.

... • When diagnostics are run on expiration of Timer T1.111.4/T19. Here, it shall take no more than 120 seconds for the STP to start link alignment.

**R9-4** covers transport facility failures, not timing facility failures (this is covered in Section 8.1.1.2.2).

### 9.1.2.2 SCCP Level

GR-246-CORE and CCITT Recommendation Q.716, *SCCP Performances* state a downtime objective for an SCCP relay point. A relay point is a signaling point in which the translation functions of the SCCP for connectionless classes are implemented. The unavailability of a relay point is the probability that it cannot perform its GTT function at a given instant of time.

**R9-5** [450] The unavailability of an SCCP relay point should not exceed $10^{-4}$ (i.e., an availability of 0.9999). This corresponds to an expected (i.e., average) total downtime of 53 minutes per year for the STPs in a given population. Note that this does not cover the STP SCCP gateway screening function.

### 9.1.2.3 ISDN-UP

Not applicable.

### 9.1.2.4 TCAP

There are currently no unavailability requirements or objectives for the STP TCAP. Further study is required to determine if they are needed.

### 9.1.3 Hardware Downtime Requirements

The requirements in this section apply to the MTP level and are for the purpose of hardware reliability modeling only.
9.1.3.1 MTP Level

9.1.3.1.1 Predicted STP Total System Downtime

The predicted STP Total System Downtime is calculated as the sum of downtime predictions (due to hardware and the OA&M activities discussed in GR-512-CORE) for each of the failure modes that cause a STP total system outage.

**R9-6** [451] The predicted STP Total System Downtime for all office configurations shall be no more than 0.6 minutes per year (due to hardware and OA&M activities).

This means that the predicted total loss of CCS capability for an STP shall be no more than 0.6 minute per year (due to hardware and the OA&M activities discussed in GR-512-CORE).

9.1.3.1.2 Predicted STP Link Downtime

The predicted STP Link Downtime is calculated as the sum of downtime predictions (due to hardware and the OA&M activities discussed in GR-512-CORE) for each of the failure modes in the STP that cause an outage of one or more links.

**R9-7** [452] The predicted STP Link Downtime shall be no more than 35 minutes per year (due to hardware and OA&M activities).

STP Link Downtime is calculated as GR-512-CORE) for each of the failure modes in the STP that cause an outage of one or more links (including those failure modes that cause a total loss of CCS capability for the STP).

Additional reliability and quality requirements are discussed in Section 11.

9.1.4 Summary

Table 9-1 summarizes the STP downtime requirements and objectives for MTP only.
Table 9-1. Summary of MTP STP Downtime Requirements and Objectives

<table>
<thead>
<tr>
<th>Node</th>
<th>Common</th>
<th>Link-Specific</th>
<th>System (Node) Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All Causes</td>
<td>Hardware</td>
<td>All Causes</td>
</tr>
<tr>
<td>STP</td>
<td>3</td>
<td>0.6</td>
<td>82</td>
</tr>
</tbody>
</table>

Notes: The values are minutes per year. The Hardware values are requirements, while the All Causes values are objectives. The System Link downtime values are the sum of the Common and Link-Specific values. They do not include the downtime of the link transport facility. N/P means not published.

Table 9-2 summarizes the STP downtime objectives for all causes.

Table 9-2. Summary of STP Downtime Requirements and Objectives for All Causes

<table>
<thead>
<tr>
<th>Node</th>
<th>SS7 Protocol Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MTP</td>
</tr>
<tr>
<td>STP</td>
<td>3 min/yr</td>
</tr>
</tbody>
</table>

Notes: The 53 min/yr objective applies only to the SCCP GTT function. It does not cover the STP SCCP gateway screening function. N/A means not applicable. U/S means under study.

9.2 STP Transport Time

The transport time of a message through an STP is specified as the cross-STP transport time. It consists of the interval beginning when the STP receives the last bit of a message from the incoming signaling link, and ending when the STP transmits the last bit of the message on the outgoing signaling link.

Cross-STP transport time can be specified as:

\[
\text{cross-STP transport time} = \text{STP node processing time} + \text{link output delay}.
\]

---

4. The term, cross-STP transport time, is used in place of the term, cross-STP delay, throughout this section.
STP node processing time consists of the interval beginning when the STP receives the last bit of a message from the incoming signaling link, and ending when the STP places the message in the output signaling link controller buffer. The supplier shall provide for STP node processing times as Section 9.2.1 describes.

Link output delay is the interval beginning when the STP places the message in the output signaling link controller buffer, and ending when the STP transmits the last bit of the message on the outgoing signaling link. Link output delay should be independent of an STP’s performance characteristics, as discussed in Section 9.2.2.

Given the STP node processing time requirements (see Section 9.2.1), the upper and lower bounds on link output delay, and the link output delay for a typical TCAP message5 (see Section 9.2.2), the upper and lower bounds on cross-STP transport times, as well as the cross-STP transport time for a typical TCAP message can be determined (see Section 9.2.3).

In Sections 9.2.1 through 9.2.3, STP transport times are stated in terms of the mean and 95th percentile values for normal loading (i.e., a fully operational network) and failure loading (i.e., where the mated STP is down and the STP in question carries the full load of the mated pair).

Additionally, there is a critical failure mode. Examples of critical failures include, but are not limited to

- Large numbers of signaling link facility failures resulting in many link changeovers and link security tasks to be processed
- Long duration and/or multiple switching office outages resulting in much network management activity
- Focused overloads during a catastrophe or other major event causing an influx of call attempts.

\[ \text{R9-8 [453] During a critical failure, the STP shall continue to operate even if it cannot meet the requirements that Section 9.2.1 describes.} \]

### 9.2.1 STP Node Processing Time

Because message length distribution has little effect on STP node processing time, STP node processing time primarily depends on the type of STP processing, the traffic mix, and the load on the STP. Table 9-3 shows STP node processing times requirements for normal and failure loading. This single set of STP node processing time requirements apply regardless of the traffic mix or of the functions that the STP has to perform on the individual

---

5. For these purposes, a “typical TCAP message” is an approximate message length (i.e., 120 octets) for TCAP messages that are being transmitted for future (near term) services (e.g., AIN 0.1).

---
messages. Thus, they apply even if the traffic mix has a high percentage of large messages and if the STP must perform many functions (e.g., GTT, gateway screening, translation type mapping, and/or ISNI) on each message.

Table 9-3. STP Node Processing Time

<table>
<thead>
<tr>
<th>Loading</th>
<th>STP Node Processing Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mean</td>
</tr>
<tr>
<td>Normal</td>
<td>43</td>
</tr>
<tr>
<td>Failure</td>
<td>80</td>
</tr>
</tbody>
</table>

R9-9 [454] The observed STP node processing time values shall be less than or equal to the corresponding STP node processing time values in Table 9-3, regardless of the traffic mix or type of STP processing required on the individual messages.

9.2.2 Link Output Delay

Link output delay is the sum of the queuing delay and message emission time. Message emission time is a function of the signaling data link speed (56-kb/s) and message length distribution.

Queuing delay is the time from when a message is placed in the output signaling link controller buffer until its first bit is transmitted. It is a function of traffic mix, message emission time, and link occupancy (a maximum of 0.4 erlang for normal mode operation and 0.8 erlang for failure mode operation). Because none of these components are based on an STP’s performance characteristics, link output delays for various scenarios can be determined independent of an STP's implementation.

Table 9-4 shows the lower bound (i.e., which assumes that all messages are 15 octets), a typical TCAP message (i.e., which assumes that all messages are 120 octets, and the upper bound (i.e., which assumes that all messages are 279 octets) of link output delay. Any other message length distribution will result in link output delay values between the lower bound and upper bound values. In Table 9-4, a link occupancy of 0.4 erlang is assumed for normal mode operation and 0.8 erlang is assumed for failure mode operation. Any decrease in link occupancy will result in a reduction in the link output delay. The type of STP processing required does not affect link output delay.
9.2.3 Cross-STP Transport Time

As mentioned previously, cross-STP transport time is the sum of the STP node processing time and the link output delay. Although several factors affect the transport time of a message through an STP, only the message length distribution and the message type distribution cannot be predetermined. Because the SS7 protocol specifies the allowable range of message lengths (i.e., 15 to 279 octets), a range of acceptable cross-STP transport times, as well as the STP transport time for a typical TCAP message, can be determined using the values from Tables 9-3 and 9-4, as Table 9-5 shows. Assuming that the STP meets the requirements from Table 9-3, the values in Table 9-5 represent the lower bound (i.e., where all messages are 15 octets), a typical TCAP message (i.e., where all messages are 120 octets), and the upper bound (i.e., where all messages are 279 octets) of cross-STP transport times.

Table 9-5. Cross-STP Transport Time

<table>
<thead>
<tr>
<th>Range</th>
<th>Loading</th>
<th>Cross-STP Transport Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Mean</td>
</tr>
<tr>
<td>Lower Bound</td>
<td>Normal</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>Failure</td>
<td>87</td>
</tr>
<tr>
<td>Typical Message</td>
<td>Normal</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>Failure</td>
<td>132</td>
</tr>
<tr>
<td>Upper Bound</td>
<td>Normal</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>Failure</td>
<td>202</td>
</tr>
</tbody>
</table>
9.3 Accuracy

**R9-10** [455] Whether the STP is carrying just its own traffic load or the full load of the mated pair while its mate is out of service, the number of errors caused by the STP shall be sufficiently small so that the STP does not exceed the following objectives by a factor of ten for MTP transfer of messages between two user parts at different nodes:

... • Undetected errors—not more than $1 \times 10^{9}$ of all messages sent will be delivered with an undetected error

... • Loss of messages—not more than $1 \times 10^{9}$ of all messages will be lost

... • Messages out of sequence—not more than $1 \times 10^{10}$ of all messages sent will be delivered out-of-sequence; this includes duplication of messages.

**R9-11** [456] These requirements do not apply during a critical failure, as Section 9.2 defines.

In practice, **R9-10** and **R9-11** are such that for reasonable periods of monitoring an STP, none of the above events should occur.

**R9-12** [457] Hardware failures in an STP shall be such that:

... • Not more than $0.2 \times 10^{11}$ of all messages sent will be delivered with an undetected error due to hardware failures in an STP

... • Not more than $0.2 \times 10^{8}$ of all messages sent will be lost due to hardware failures in an STP

... • Not more than $0.2 \times 10^{11}$ of all messages sent will be delivered out-of-sequence; this includes duplication of messages.
Figure 9-1. Access and Backbone Network

*THE BACKBONE NETWORK MAY CONSIST OF A NUMBER OF NETWORKS THAT ARE INTERCONNECTED TO PROVIDE A SIGNALING PATH.
10. Environmental Requirements

10.1 Power

R10-1 [458] The STP shall be designed to obtain power from a nominal -48 Vdc CO power system. Refer to GR-513-CORE, LSSGR: Power, Section 13, for power system requirements.

10.2 Equipment

GR-63-CORE, Network Equipment-Building System (NEBS) Requirements: Physical Protection, specifies equipment requirements for all systems to be deployed in COs.

R10-2 [459] All equipment shall satisfy the spatial and environmental requirements in GR-63-CORE.

10.3 Electromagnetic and Electrical Environment

GR-63-CORE provides requirements to ensure that a switch complies with Federal Communications Commission (FCC) specifications, that it has intrasystem electromagnetic compatibility, and that intersystem electromagnetic compatibility exists between systems in the CO. It also includes electrical safety requirements.
11. Quality

11.1 Introduction

This section provides an overview of the generic Reliability and Quality (R&Q) requirements for the STP. The intent of these generic R&Q requirements is to assist the Bccs in continuing to provide excellent service, reducing maintenance costs, and providing stable and dependable system operation.

FR-796, Reliability and Quality Generic Requirements (RQGR), is a collection of Bellcore R&Q requirements presenting Bellcore’s view of proposed generic requirements that are needed to help ensure the uninterrupted performance, reliability, and quality of products intended for use as network elements in a typical Bcc network. A brief description of each document in the RQGR collection appears in GR-874-CORE, An Introduction to the Reliability and Quality Generic Requirements (RQGR).

Among all the R&Q requirements documents, TR-NWT-000284, Reliability and Quality Switching Systems Generic Requirements (RQSSGR), particularly gives the R&Q requirements for switching systems, including the STP. In this section, only the key items of the RQSSGR are listed. Further details are in the RQSSGR and its references.

Section 9.1 contains specific STP reliability objectives. Section 12 contains additional R&Q requirements related to that topic.

11.2 Reliability and Quality Switching Systems Generic Requirements

In addition to the quantitative reliability performance objectives stated in Section 9.1, qualitative and analytical generic R&Q requirements and objectives applicable to network system design, manufacture, and support are provided or referenced in the RQSSGR. These generic reliability and quality requirements are intended to help ensure that network systems provide stable and dependable operation throughout their service life, and that maintenance and administration costs are continually reduced. The RQSSGR also provides requirements for developing reliability models appropriate for analyzing system architecture and recovery designs against the quantitative objectives.

The RQSSGR is subdivided into three major categories:

- System Design and Architecture
- Manufacturing and Production
- In-Service Performance and Product Support.

Each category is summarized by the following.
11.2.1 System Design and Architecture

The System Design and Architecture section of the RQSSGR addresses the following areas of system design and architecture requirements:

- System Reliability Performance
- Hardware Design and Architecture
- Software Design and Architecture
- Conformance to Requirements.

11.2.2 Manufacturing and Production

The Manufacturing and Production section of the RQSSGR describes the requirements for incorporating R&Q practices in the manufacturing and production phases of the product life cycle. These phases also require that certain procedures be used to help ensure the R&Q of the shipped product. The areas of the requirements include the following:

- Testing
- Component and Device Reliability
- Product Inspection
- Supplier Data Program
- Quality Program
- Manufacturing Program
- Periodic Product and Process Requalification.

11.2.3 In-Service Performance and Product Support

The In-Service Performance and Product Support section of the RQSSGR provides in-service performance and product support requirements for switching network elements. The requirements for in-service performance monitoring and practices are described. The product support requirements and objectives address the following elements of a product program:

- Reliability and Quality Cost
- Engineering and Ordering
- Installation
- First Office Application
• Training
• Technical Assistance
• Deliverable Customer Documentation
• Product Change Procedures
• Repair
• Supplier’s Spares Plan
• Engineering Complaints.
12. Supplier Support

R12-1 [460] The STP vendor shall meet the supplier support generic requirements published in:

... • GR-454-CORE, Generic Requirements for Supplier-Provided Documentation

... This document describes Bellcore's view of proposed generic requirements for documentation that suppliers should provide with Network Elements (NEs) and Network Systems (NSs) that a typical Bcc purchases to meet its needs.

... • GR-839-CORE, Generic Requirements for Supplier-Provided Training

... This document provides Bellcore's view of proposed generic requirements that affect supplier-provided training. It documents the generic requirements from the needs assessment stage through the development, delivery, implementation, and evaluation phases, and addresses existing training as well as training to be developed.

... • TR-NWT-000840, Supplier Support Generic Requirements (SSGR)

... This document addresses the following aspects of supplier support:

... — Engineering and Ordering
... — Installation and Removal
... — First Application
... — Technical Assistance
... — Repair and Return
... — Spares.

Additional supplier support requirements specific to STPs are stated below.

12.1 Documentation on Operations

R12-2 [461] Work position manuals shall describe each work position, installation procedures, how to set options and parameters, how to use the work station, and fields in each screen.

R12-3 [462] In addition, detailed descriptions shall be provided for STP output messages.
12.2 Software Documentation

R12-4 [463] A set of clearly defined and documented Regression Test and Acceptance Procedures shall exist for running basic sanity tests on the software on completion of installation and initialization activities.

R12-5 [464] Documented RC&V Procedures are required for all provisioning activities defined in Section 5.2.

R12-6 [465] As discussed in GR-282-CORE, *Software Reliability and Quality Acceptance Criteria (SRQAC)*, for each new software release or fix, lists shall be provided that include all modules in the load, all problems fixed in the release, all known problems in the release, and all modules affected by the change. Changes to all affected documentation shall also be included.
Appendix A: Changes for E-Links and Complex Network Architectures

Significant changes were recently introduced into the SS7 protocol by the ANSI T1S1.3 standards working group. They were motivated by an impending introduction of E-links into CCS networks and by the appearance of more complex CCS network architectures. These changes appear for the first time in Revision 2 of GR-246-CORE. They are summarized in Appendix A.

• Changes in Transfer-Prohibited Procedure

Changes in the transfer-prohibited procedure were introduced to deal with the problem of possible circular routing when three or more route priorities may be present at an STP for a given destination. It turns out that to avoid circular routing under these circumstances, additional preventive TFP or TCP messages must be sent. (TFP/TCP messages sent to prevent circular routing are referred to as “preventive” TFP/TCPs.)

Two additional rules for sending preventive TFP/TCP messages are necessary. The need for the first rule is illustrated in Figure A-1. As shown in that figure, when link set failures between signaling end-point (SEP) A and STPs occur in the sequence indicated by the numbered X’s, looping of messages destined for A will occur as shown by the arrows if the following rule for sending preventive TFP/TCP messages were not introduced:

When an STP diverts traffic from an unavailable route to a route of lower priority, preventive TFP/TCPs must be sent to all accessible adjacent STPs on alternate routes of higher priority than the new route to the affected destination.

The need for the second additional rule in some network architectures is illustrated in Figure A-2. As shown in that figure, when all three link sets from SEP A to STPs fail in any sequence, looping of messages destined for A will occur as shown by the arrows if the following STP capability for sending preventive TFP/TCP messages were not introduced:

An STP shall provide the ability to provision a list of selected adjacent STPs, on a per-destination basis, that require a preventive TFP/TCP. For a particular destination X, such a list specifies, first, a route priority (i.e., cost in the terminology of Section 4.2.3.2.1) and, second, a set of adjacent STPs. (It is necessary to include a route priority because the action mentioned in the next sentence should not be taken when traffic is diverted to the C-link set.) When traffic for X is diverted from a higher priority route to a route of the priority specified on the list, the STP shall send a preventive TFP/TCP regarding X to the accessible STPs on the list.

For the network corresponding to Figure A-2, the list of selected adjacent STPs would have to be provisioned in at least one of the STPs, although for optimal routing...
efficiency it should be provisioned at all three STPs. The list will contain a Point Code of the STP corresponding to the 3rd priority route.

*Note, the second rule is not included in the requirements since Bcc networks do not plan to utilize the architectures or routing schemes which make that rule necessary.*

For more information on additional rules for sending preventive TFP/TCP messages see Section 4.2.4.12.2.

Since circular routing may arise when a preventive TFP/TCP is not acted upon, an STP sending a preventive TFP/TCP must also discard messages addressed to the affected destination and received from an adjacent STP to which a preventive TFP/TCP was sent. The STP may also need to resend a preventive TFP/TCP. For more information see Section 4.2.4.12.2.

- **Changes to Transfer-Restricted Procedure**

  A change in the transfer-restricted procedure is necessary because when three or more route priorities may be present at an STP for a given destination, traffic may be diverted to a higher priority route but not to a normal route. If routes of no more than two priorities may be present, this is not possible. According to a new rule for sending TFR/TCR message, when traffic for a destination is diverted to a higher priority route, but not the normal route, a TFR/TCR message regarding that destination must be sent to the adjacent STP on the previously used route to the destination.

- **Changes to Signaling-Route-Set-Test Procedure**

  Changes in the signaling-route-set-test procedure are necessary because of introduction of additional criteria for sending preventive TFP/TCP messages. When a signaling-route-set-test message is received from an STP to which a preventive TFP/TCP regarding the tested destination was sent, such signaling-route-set-test message must be treated differently than when it is received from an STP to which a preventive TFP/TCP was not sent. For more information, see Section 4.2.4.15.4.
Figure A-1. Message Looping without the 1st Additional Rule for Preventive TFP/TCPs

Solid lines between signaling end-point (SEP) A and STPs B and C represent A-link sets, dotted lines between SEP A and STPs D and E represent E-link sets. Numbered X’s crossing the A-and E-link sets denote the sequence of link set failures. Arrows denote the looping of messages destined for SEP A that will occur after all four link sets between A and STPs fail in the sequence indicated by the numbered X’s without the first additional rule for sending preventive TFP/TCP messages.
Figure A-2. Message Looping without the 2nd Additional Rule for Preventive TFP/TCPs

Numbers on link sets around each STP represent routing priorities towards signaling endpoint (SEP) A. When all link sets between SEP A and STPs fail in any order, looping of messages destined for SEP A will occur as shown by the arrows in the absence of an additional capability at STPs to send TFP/TCP messages as discussed in the main text.
Appendix B: STP Requirements for Toll-Free Service

B.1 Introduction

The role of the STP in transferring messages for Toll-Free Service to provide MTP message handling and SCCP routing is described in Section 4. Messages for Toll-Free Service will be transferred to the STP by an SSP. After performing the global title translation, the STP should route the message to a SCP node where the Toll-Free Service database application resides.

This GR states procedures for routing all messages and for performing global title translations for any service that requires specialized routing. The STP operations requirements aim to enable and maintain the STP’s capabilities for handling all messages. This section illustrates the application of the functions described in this GR to serve the needs of Toll-Free Service.

Section B.2 contains formatting information for the parts of the Toll-Free Service message that the STP is required to process in transferring the Toll-Free Service message. Operations requirements in Section B.3 detail information specific to provisioning and administering the STP for Toll-Free Service capabilities.

B.2 MTP and SCCP Message Formats for Toll-Free Service

RB-1 [466] Three functional components of the SS7 protocol are involved in Toll-Free Service messages: the MTP, which shall provide the basic message routing capabilities on a link-by-link basis; the SCCP, which defines the type of end-to-end transport service that shall be used for the message in addition to providing specialized routing capabilities; and TCAP, which shall provide the application data required for processing Toll-Free Service calls.

This section demonstrates how MTP and SCCP information shall be encoded for Toll-Free Service messages requiring global title translation at an STP.

B.2.1 MTP Message Formats

Each Toll-Free Service message contains the following MTP information, as shown in Table B-1.
Table B-1. MTP Message Information

<table>
<thead>
<tr>
<th>h</th>
<th>g</th>
<th>f</th>
<th>e</th>
<th>d</th>
<th>c</th>
<th>b</th>
<th>a</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>BIB</td>
<td>Backward Sequence Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>FIB</td>
<td>Forward Sequence Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>Spare</td>
<td>Length Indicator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>F</td>
<td>Signaling Information Field</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>Check Bits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A. **Flag**—A unique 8-bit pattern (01111110) is used to delimit the SS7 message. To avoid misinterpreting information octets, a “0” bit is inserted into the bit stream after every sequence of five consecutive “1” bits that are not part of a delimiting flag as each message is transmitted. These “0” bits should then be deleted at the receiving signaling terminal.

B. **Backward sequence number and Backward Indicator Bit (BIB)**—This field is used with forward sequence information to provide signal unit sequence control and acknowledgment functions. The sequence information is important to message flow control on the individual signaling links used to transmit SS7 messages.

C. **Forward sequence number and Forward Indicator Bit (FIB)**—As described above.

D. **Length indicator**—This field indicates the number of octets (3-63) in the signaling information field. If the signaling information field spans more than 62 octets, the length indicator is set to 63 (coded as 111111). Length indicator values of 0, 1, or 2 are used for fill-in signal units and link status signal units.

E. **Service information octet**—This field contains a service indicator (bits d-a) that indicates the MTP-user part involved in the message; here, the SCCP (code “0011”). The subservice field (bits h-e) provides a network indicator, and for national network messages (as indicated by code “10” in bits h-g), message priority. All Toll-Free
Service messages are assigned priority 1 (code “01” in bits f-e), where priority 3 is the highest priority assigned to SS7 messages. MTP message priority does not determine which messages are processed first when received at a node, but is used instead to determine which messages should be discarded when the SS7 network experiences congestion.

F. **Signaling information field**—This is a variable length field that carries the information generated by a user part. The format and codes for the signaling information field are defined separately for each user part. The field may contain up to 272 octets of information. For Toll-Free Service messages, the signaling information field will contain SCCP and TCAP message information.

G. **Check bits**—Each signal unit has a 16-bit cyclic redundancy check field for error detection.

### B.2.2 SCCP Message Formats

#### B.2.2.1 Overview

All Toll-Free Service messages are encoded in SCCP Unitdata messages, as shown in Table B-2. Because SCCP procedures depend on the nature of application data being transported, the SCCP message parameters vary from one Toll-Free Service message to another. SCCP information is encoded in the signaling information field of the SS7 message.
### Table B-2. SCCP Unitdata Message Information

<table>
<thead>
<tr>
<th></th>
<th>h</th>
<th>g</th>
<th>f</th>
<th>e</th>
<th>d</th>
<th>c</th>
<th>b</th>
<th>a</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DPC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>OPC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>Spare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
<td>Options</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Pointers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SCCP Calling Party Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SCCP Calling Party Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

First bit transmitted

Signaling Link Selection
A. Routing label:
   1. DPC—The SS7 address for the recipient node of the message
   2. OPC—The SS7 address for the node sending the message
   3. Signaling Link Selection (SLS) code—A code that directs the message to a particular signaling link for transmission.

B. Message type. The SCCP Unitdata message is used to transmit Toll-Free Service information.

C. Protocol class parameters. Protocol class 0 (connectionless service, no message sequencing required) is used for all Toll-Free Service messages. The protocol class is indicated in bits d-a of the protocol class parameter field. Bits h-e indicate any options that should be used with the protocol class. For example, the options might indicate that the receiving node of a message should notify the sending node if it is unable to deliver the message to the SCCP user.

D. Pointers. The pointers identify the location of the beginning of variable length SCCP parameters. Three pointers are used in Unitdata messages:
   1. Pointer to the beginning of the SCCP called party address field
   2. Pointer to the beginning of the SCCP calling party address field
   3. Pointer to the beginning of the data field.

E. SCCP called party address. The contents of the SCCP called party address field indicate the functional component of the SS7 protocol that should be used as the basis for decoding information in the data field. The field includes:
   1. A length indicator that explicitly describes (in binary coding) the number of octets of information in the field.
   2. Address indicator that describes the contents of the SCCP called party address. Bit a indicates whether an SSN is present. The SSN identifies the SCCP user that will receive the message. Bit b indicates whether an SPC is present. Bits c-f indicate whether a global title is present and, if so, how the global title is coded. The global title is a nonsignaling network address that can be used to determine the identity of an SCCP user. Bit g indicates which information in the SCCP called party address should be used for routing the message. Bit h indicates whether the SCCP called party address is coded according to international specifications.
   3. The SCCP called party address is formatted as indicated by the address indicator.

F. SCCP calling party address. The SCCP calling party address field provides information about the SCCP user that originated the message and is formatted identically to the SCCP called party address.
G. Data. The data field contains the following specific application information necessary for Toll-Free Service processing:

1. A length indicator that is the binary-coded representation of the number of octets of information contained in the data field
2. Data information for Toll-Free Service, formatted according to TCAP procedures.

B.2.2.2 Unitdata Messages the STP Receives from the SSP

The Toll-Free Service messages sent by the SSP to the STP for global title translation contain the following information, as shown in Table B-3.

A. Routing label:

1. The DPC identifies the STPs that the SSP has indicated should perform global title translation.
2. The OPC identifies the SSP sending the Toll-Free Service message.
3. The SLS is chosen by the SSP to permit load sharing of messages on signaling links.

B. The message type, 00001001, indicates a Unitdata message.

C. The code “0000” in bits d-a of the protocol class parameters field indicates that the Unitdata message uses protocol class 0. The code “0000” in bits h-e indicates that no special options should be applied to the message.

D. Pointers:

1. The SCCP called party address field begins in the third octet following its pointer.
2. The SCCP calling party address field begins in the ninth octet following its pointer.
3. The data field begins in the 14th octet following its pointer.

E. The SCCP called party address field provides the following information:

1. The called party address field contains five octets of information.
2. The address indicator indicates that the SCCP called party address is coded according to U.S. rather than international standards (code “1” in bit h). In addition, the address indicator indicates that the receiving node should perform global title translation (code “0” in bit g). The global title indicator is coded “0010” in bits f-c to indicate that the global title would include a translation type and a global title address. The address information should also include an SSN (code “1” in bit a), but no PC (code “0” in bit b).
Table B-3. SCCP Information for Unitdata Messages Sent by SSP to the STP

<table>
<thead>
<tr>
<th></th>
<th>h</th>
<th>g</th>
<th>f</th>
<th>e</th>
<th>d</th>
<th>c</th>
<th>b</th>
<th>a</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DPC</td>
<td></td>
<td></td>
<td>First bit transmitted</td>
</tr>
</tbody>
</table>
|   |   |   |   |   |   |     |   |   | ----->
| 2 |   |   |   |   |   | OPC |   |   |
| 3 |   |   |   |   |   |     |   |   | Spare | Signaling Link Selection |
| B | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| C | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| D | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
|   | 2 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
|   | 3 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| E | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
|   | 2 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
|   | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 |   |   |   |   |   |     |   |   | Translation Type |
|   |   |   |   |   |   | 2nd NPA digit | 1st NPA digit |
|   |   |   |   |   |   | 1st NXX digit | 3rd NPA digit |
|   |   |   |   |   |   | 3rd NXX digit | 2nd NXX digit |
| F | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
|   | 2 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
|   | 3 |   |   |   |   | SSP Toll-Free Service SSN |
| 4 |   |   |   |   |   |     |   |   | Point Code of SSP |
| G | 1 |   |   |   |   |     |   |   | Length Indicator |
|   | * |   | * |   |   |     |   |   | |
| 2 |   | Data |   |   |   |     |   |   | |
|   |   | * | * |   |   |     |   |   | * |
3. The SSN included in this message is the null SSN. This field serves as a place holder for the meaningful SSN that will be carried after the global title translation is performed at the STP.

4. The translation type is used by the STP to identify which translation table should be used to obtain SCCP routing information based on the global title. The coding of this 8-bit field is based on which Toll-Free Service NPA was dialed. Each Toll-Free Service NPA (or AIN trigger for Toll-Free Service) may have a separate translation type or they may share a translation type, as provisioned by the Bcc at the SSP.

5. The global title value is contained in a 3-octet field and is the binary-coded form of the Toll-Free Service NPA-NXX digits dialed by the caller.

F. The SCCP calling party address field provides the following information:

1. The calling party address field contains five octets of information.

2. The address indicator indicates that the including an SSN (“1” in bit a) and a PC (“1” in bit b). The SCCP calling party address field does not contain a global title (code “0000” in bits f-c), and the response message should be returned to the calling SCCP user indicated by the PC and SSN provided (code “1” in bit g). The SCCP calling party address is coded according to U.S. standards (code “1” in bit h).

3. The SSN indicates the Toll-Free Service feature has initiated the Unitdata message using the TCAP part of the SS7 protocol. Each Toll-Free NPA (or Toll-Free trigger, using AIN) may have a separate SSN or they may share a SSN. Inclusion of this information allows the response message to be returned efficiently to Toll-Free Services processing at the SSP.

4. The PC identifies the SSP to which the Toll-Free Service response message should be returned.

G. The Unitdata message data field is formatted as described within TCAP procedures.

B.2.2.3 SCCP Information for Toll-Free Service Messages after Global Title Translation

The SCCP information content of Toll-Free Unitdata messages formatted by the SSP is changed by the STP when it performs global title translation, as shown in Table B-4.
### Table B-4. SCCP Information for Toll-Free Service Messages After Global Title Translation

<table>
<thead>
<tr>
<th></th>
<th>h</th>
<th>g</th>
<th>f</th>
<th>e</th>
<th>d</th>
<th>c</th>
<th>b</th>
<th>a</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DPC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

#### Column Headers
- **First bit** transmitted
- **DPC** transmitted
- **OPC** transmitted
- **Spare**
- **Signaling Link Selection**
- **Toll-Free Database SSN**
- **Translation Type**
  - 2nd NPA digit
  - 1st NPA digit
  - 1st NXX digit
  - 3rd NPA digit
  - 3rd NXX digit
  - 2nd NXX digit
- **SSP Toll-Free SSN**
- **Point Code of SSP**
- **Length Indicator**
  - *
  - *
  - Data
  - *

---

```
First bit transmitted
----->
```

---

```
<p>| | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DPC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>G</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
A. Routing label:
   1. The DPC identifies the SCP node at which the Toll-Free application that will
      process the Unitdata message is located.
   2. The OPC identifies the STP that performed the global title translation.
   3. The SLS field value is derived from the value contained in the message received
      from the SSP. The STP alters the SLS only if it performs SLS rotation before
      sending the message to the SCP.
B. The message type, 00001001, indicates a Unitdata message.
C. The code “0000” in bits d-a of the protocol class parameters field indicates the
   message uses protocol class 0. The code “0000” in bits h-e indicates no special options
   apply to the message.
D. Pointers:
   1. The SCCP called party address field begins in the third octet following its pointer.
   2. The SCCP calling party address field begins in the ninth octet following its pointer.
   3. The data field begins in the 14th octet following its pointer.
E. The SCCP called party address field provides the following information:
   1. The called party address field contains six octets of information.
   2. The address indicator indicates that the Unitdata message contains a global title
      (code “0010” in bits f-c) and an SSN (code “1” in bit a), but does not include a PC
      (code “0” in bit b). The coding of “1” in bit g indicates that the message should be
      routed to the SCCP user associated with the SSN. The SCCP called party address
      is coded according to U.S. standards (code “1” in bit h).
   3. The SSN identifies the Toll-Free Service database application at the SCP node that
      should process the Unitdata message.
   4. The global title information, including translation type and global title address,
      should be identical to that contained in the Unitdata message received from the
      SSP. This allows global title information to be returned with Unitdata service
      messages so that the STP can evaluate the source of SCCP routing errors more
      efficiently.
F. The SCCP calling party address field should be identical to that provided in the Toll-
   Free Service query message sent from the SSP to the STP.
G. The message data field is formatted as described within TCAP procedures. The STP
   neither reads nor alters information in the data field as part of performing global title
   translation.
B.3  Operations

The operations requirements for implementing the global title translation for Toll-Free Service in the STP are in the areas of provisioning and administration.

B.3.1  Provisioning

RB-2  [467] Provisioning the STP for Toll-Free Service shall follow the requirements in Section 5.2.

This section provides Toll-Free Service-specific data for the entity set “Ordered Global Title Translation” in the “User’s View of Entity Sets.”

TOLL FREE GLOBAL TITLE TRANSLATION

This entity set forms the translation table(s) for Toll-Free Service global titles. This entity set is formed by associating the global title contained in Toll-Free Service messages with the addressing for the Toll-Free Service database application at the SCP node. The “Cost” attribute indicates the relative desirability of the translation object for each NXX.

ATTRIBUTES

Global Title Address—INT(6); corresponds to the 3-octet field for the global title address in the SCCP called party address field. These are the dialed Toll-Free Service NPA-NXX digits.

Point Code—INT(9); the internal SS7 designation of the SCP to which the Toll-Free Service message should be routed. It is formed by concatenating the three decimal digits representing the binary number contained in each of the three octets in the SS7 designation.

CLLI—CHAR(11); the CLLI code of the SCP node.

Subsystem Number—INT(3); the identification of the Toll-Free application software at the SCP. It is the decimal representation of the binary number to be placed in the 1-octet field in the SCCP called party address field. Note, there may be more than one SSN at the SCP that provides Toll-Free application software.

Cost—INT(2); the weighting factor applied to the object. Objects of equal desirability are assigned equal costs. The costs will be assigned values from 00 to 99, representing the most desirable to the least desirable, respectively.

KEY ATTRIBUTES: Global Title Address—CLLI—Subsystem Number—Global Title—Point Code—Subsystem Number.
B.3.2 Administration

RB-3 [468] For administrative purposes, two additional measurements shall be provided in the “System Total” set of traffic measurements:

... • Number of Toll-Free Service global title translations performed (using a Toll-Free Translation Type)

... • Number of Toll-Free Service global title translations unable to perform (using a Toll-Free Translation Type).

Note, if a different translation type is used for a new NPA for Toll-Free Service, then the STP will provide the per translation type measurements in Section 6.4.3.

If more than one NPA uses the same translation type, it is not expected that these measurements will be separated by NPA code; per translation type measurements will be sufficient.
Appendix C: STP Requirements for Gateway Function

C.1 Introduction

The Gateway Function at an STP consists of several components: gateway screening, translation type mapping, and gateway data collection. Translation type mapping is discussed separately in Appendix F. Gateway data collection falls into two categories: measurements that monitor gateway STP and gateway link set activity levels, and those that monitor the gateway screening process.

Gateway screening is a process during which an STP checks the contents of the incoming message and determines whether the message should be accepted or rejected (i.e., whether it is authorized) based on criteria specified by CCS network administration. The gateway screening process allows network administrators to control the flow of SS7 messages into or through a signaling network. If a message is accepted, it is passed to the MTP or SCCP for further processing (e.g., routing). If a message is rejected, it is discarded. After the rejection, an STP may generate an event report to an Operations System (OS). Also, except for emergencies, an STP always takes measurements of rejections.

In most cases, gateway screening will be applied at gateway STPs to messages received from other networks. It is possible, however, that gateway screening will be applied at non-gateway STPs, or at gateway STPs but to intranetwork link sets. Thus, the term “gateway screening” should not be interpreted as the screening applied only at gateway STPs to messages arriving from another network.

The objectives of this Appendix are to present an overview of gateway screening and to state requirements for the gateway function. To summarize the required gateway screening capability, an STP must allow a network administrator to provision sequences of screening steps to be performed for messages arriving at the STP on any given link set. A sequence of screening steps to be performed for a particular message is a function of the attributes or parameter values in that message and the link set on which it arrives. This screening capability allows a network administrator to apply different screening criteria to different link sets and different messages (e.g., from different originating networks).

This Appendix may be read as an introduction to GR-778-CORE. These documents describe the SEAS-STP interface for the gateway function and messages exchanged between SEAS and an STP associated with that function. They contain all but new gateway function requirements stated in this Appendix and also present additional requirements on validations of provisioned data, data collection, and reports of message screening rejections.

The remainder of this appendix is organized as follows.

Section C.2 presents an overview of the gateway screening process.

Section C.3 describes the gateway screening tables.
Section C.4 states the motivation for new gateway screening requirements. The requirements themselves appear in Section C.5.

Section C.5 presents requirements for the gateway function including gateway screening requirements.

Section C.6 discusses the measurements associated with the gateway function.

Section C.7 considers STP performance associated with gateway screening.

### C.2 Overview of the Gateway Screening Process

An STP performs gateway screening based on the link set over which a message arrived and on the MTP, SCCP, and ISDNUP parameters in the received message. A network administrator shall be able to specify screening criteria for any link set, intranetwork or internetwork.

A conceptual view of how gateway screening functionality fits with MTP and SCCP functions for messages arriving at an STP is depicted in Figure C-1 (see also Figure 5/T1.111.1 in GR-246-CORE and Figure C-2 in this GR). As this figure shows, MTP screening occurs conceptually before MTP discrimination and distribution functions, SCCP screening occurs both before and after those MTP functions, and ISDNUP screening occurs before the MTP routing function. The reason that SCCP screening must be performed in two stages is that the screening on the Called Party Address must take place after the SCCP routing (i.e., routing by means of Global Title Translation or ISNI) because this screening is applied to the newly derived destination address while screening of the remaining SCCP fields occurs before SCCP routing.

The fields in an SS7 message that may be checked during the screening process are:

- **MTP Parameters:**
  - Originating Point Code (OPC)
  - Destination Point Code (DPC)
  - Service Information Octet (SIO)
  - Affected Destination in MTP Network Management messages.

- **SCCP Fields:**
  - Calling Party Address (CgPA)
  - Message Type (UDT, XUDT, etc.)
  - Called Party Address (CdPA) (including Translation Type)
  - Affected Point Code/Subsystem Number (PC/SSN) in SCCP Management messages.
• ISDNUP Parameters:
  — Message Type (e.g., IAM, ACM, etc.)

It is convenient to view the gateway screening process as a flowchart or more precisely as a directed graph without cycles. Each screening check performed for an individual message, e.g., a check whether the OPC in the received message is allowed or whether the DPC is disallowed, will be referred to as a step. At the end of each step, there is either a pointer to another step or a “STOP”, “FAIL”, or “IGNORE” pointer indicating that screening of the current message has been completed. A “STOP” pointer indicates that screening should stop and the message should be passed to MTP or SCCP for further processing. A “FAIL” pointer indicates that the message is rejected and should be discarded and this event is reported. An “IGNORE” pointer is the same as a “FAIL” pointer, except that the event is NOT reported.

A pointer to the next step generally depends on the values of parameters just checked. For example, for one OPC, the next step may be to check whether the DPC is disallowed, and for a different OPC, the next step may be to check whether the SIO is allowed. Possible choices for the next step are restricted. For example, after a check for an allowed OPC, the next step can be a check for the allowed DPC, but after a check for an allowed DPC, the next step cannot be a check for an allowed OPC. All possible values for the next screening step pointer are identified in the next section. See also Figures C-2 and C-3.

Each screening step has an associated set of provisioned data which determines the screening applied to the message. Each particular combination of message parameters included within a provisioned data set will be referred to as a row. The only screening actions that an STP may apply independently of the provisioned data are the error detection and data validation procedures described in GR-778-CORE. In each screening step, parameters in the received message are compared against the values in the provisioned data to determine how to proceed with message processing.

A collection of provisioned data sets associated with screening steps of the same type, e.g., those that check for an allowed OPC, will be referred to as a screening table. The terms “screening table” and “row” are used for the purpose of describing provisioned screening data and their use is not intended to imply a particular implementation of internal STP storage of such data. Since screening tables completely specify the screening process, further discussion of gateway screening throughout this Appendix will be primarily in terms of these tables. Such description permits a rapid association of material in this Appendix with corresponding provisioning requirements in GR-778-CORE.

### C.2.1 Screening Table Structure

Each screening table consists of two types of information: screening and structural. Screening information identifies SS7 message fields to be screened and valid or invalid values for those fields. Structural information provides the means to specify sequences of
screening steps to be applied to received messages. As discussed above, these sequences of steps define a hierarchical tree.

Structural information consists of entry point references and pointers. Pointers contain table names and entry point references. As discussed above, a pointer may also indicate STOP, FAIL, or IGNORE.

A screening table may be empty or it may consist of one or more data sets corresponding to different screening steps. Each data set has a unique entry point reference associated with it. See Tables C-1 and C-2 as examples. (For conciseness in these example Tables, a “*” is being used to indicate the entire allowed range of the parameter.)

### Table C-1. Example of Allowed OPC Table

<table>
<thead>
<tr>
<th>Entry Point Reference</th>
<th>NI</th>
<th>NC</th>
<th>NCM</th>
<th>Next Step Pointer</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>246-253</td>
<td>*</td>
<td>*</td>
<td>Blocked OPC, 400</td>
</tr>
<tr>
<td>200</td>
<td>244</td>
<td>*</td>
<td>*</td>
<td>STOP 121-255</td>
</tr>
<tr>
<td></td>
<td>245</td>
<td></td>
<td></td>
<td>Blocked OPC, SK5</td>
</tr>
</tbody>
</table>

NI denotes Network Identifier, NC - Network Cluster, NCM - Network Cluster Member

### Table C-2. Example of Blocked OPC Table

<table>
<thead>
<tr>
<th>Entry Point Reference</th>
<th>NI</th>
<th>NC</th>
<th>NCM</th>
<th>Next Step Pointer</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>(if match 253 is not found)</td>
<td>11</td>
<td>121-255</td>
<td>Allowed SIO, 700 FAIL</td>
</tr>
<tr>
<td>SK5</td>
<td>(if match 244 is not found)</td>
<td>157</td>
<td>233-250*</td>
<td>Allowed SIO, 2200 FAIL</td>
</tr>
<tr>
<td></td>
<td>245</td>
<td>241</td>
<td></td>
<td>FAIL</td>
</tr>
<tr>
<td></td>
<td>245</td>
<td>242</td>
<td></td>
<td>FAIL</td>
</tr>
</tbody>
</table>

NI denotes Network Identifier, NC - Network Cluster, NCM - Network Cluster Member

Screening tables fall into two types: allowed and blocked. Example of the user's view of the allowed type is in Table C-1 and of the blocked type in Table C-2. For each data set corresponding to a screening step, the first row contains an entry point reference. A data set may consist of one or more rows. Each row for a data set in the “Allowed OPC” table, and in any table specifying allowed parameters, ends with the next step pointer or STOP. The first row of a data set in the “Blocked OPC” table, and in any table specifying blocked parameters, does not contain any screening parameters but only a pointer to the next step or STOP, which an STP refers to after all screening data has been scanned; every
subsequent row ends with the FAIL pointer. The presence of the first row in a table specifying blocked parameters prevents this table from rejecting messages whose parameters match no subsequent row of this table.

STP actions (as viewed by the user) for a particular screening step depend on the type of table associated with the step:

- When the table type is *allowed*, the STP scans the data set corresponding to the current screening step. If the STP finds a match between message parameter(s) and provisioned value(s) in a row of the screening table, the received message is allowed (unless the next screening step is IGNORE). The STP then checks the pointer to the next screening step specified for that row. If the pointer says STOP, no further screening is applied and the message is accepted; if the pointer says IGNORE, the message is discarded but no event report is made; otherwise, the next step is taken as indicated by the pointer. If the STP has scanned all rows in the data set and the message has not been accepted, the message is rejected. (As explained below, the rows may be scanned in any order.)

- When the table type is *blocked*, the STP scans the provisioned data set corresponding to the current screening step. When it finds a matching entry indicating that the parameter in the received message is disallowed, the message is rejected because the next step is always provisioned as FAIL. If the STP has scanned all rows and the message has not been rejected, it checks the pointer to the next step specified in the first row of the data set. If the pointer indicates STOP, no further screening is applied and the message is accepted; otherwise, the next screening step is taken as indicated by the pointer. Just two screening tables in this category exist: Blocked OPC and Blocked DPC.

Entries with overlapping data are not allowed in the same data set. For example, an STP shall not allow one entry (i.e., table row) with Network Identifier (NI) range specified as 211-240 and another entry with the NI range 231-250 within the same data set in an Allowed OPC table. Since overlapping data are not allowed, provisioned entries (equivalent to rows in Tables C-1 and C-2) for a particular screening step may be scanned in any order.

### C.2.2 Gateway Link Set Table

There is another provisioned table at an STP performing gateway screening which is referred to as the Gateway Link Set table. This table specifies the link sets for which the STP should perform gateway screening. Each link set may be intranetwork or internetwork. Although the table does not specify any SS7 message parameters to be screened, it is still referred to as a gateway screening table.

Each entry in the Gateway Link Set table consists of two items. In addition to the link set name (i.e., link set ID), there is a pointer to the first screening step to be applied to messages
received over the link set. The pointer determines possible sequences of steps that will be applied to messages arriving over the link set. Possible first steps for any link set are:

- Allowed OPC
- Blocked OPC
- Allowed SIO
- Allowed DPC
- Blocked DPC
- STOP (e.g., in case a Bcc wishes to collect gateway measurements for a particular link set without performing any screening for messages arriving over that link set).

### C.2.3 Pre-GTT and Post-GTT Gateway Screening

A specific requirement for when an STP should interrupt gateway screening to perform any needed SCCP routing is not stated. The break point can occur at any time before screening is performed for the Called Party Address (CdPA) in the received message. However, if global title translation is needed, it may be most efficient to perform the SCCP routing immediately before CdPA screening because the STP will not then perform SCCP routing for a message that it will subsequently reject in a screening step preceding CdPA.

### C.3 Description of Gateway Screening Tables

The following subsections describe gateway screening tables for MTP, SCCP, and ISDNUP fields.

For each gateway screening table, the following information is provided:

- Provisioned screening data
- Possible next steps.

Provisioned structural data consisting of entry point references and next step pointers is not mentioned.

The purpose of each table is usually evident from its name, but in a few cases when it is not, the purpose is stated explicitly. Explanatory remarks appear at the end of table descriptions.

### C.3.1 MTP Screening Tables

Figure C-2 depicts the flow of MTP gateway screening. Exits from the right in Figure C-2 feed into the corresponding entry points in Figure C-3.
1. **Gateway Link Set**

   **Purpose:**
   
   This screening table specifies link sets for which gateway data collection is performed and screening criteria may be specified. Although the table does not specify any SS7 message parameters to be screened, it is still referred to as a gateway screening table and is considered to be one of MTP screening tables.

   **Provisioned Data:**
   
   Link Set Name
   Link Set Group Identifier

   **Possible Next Steps:**
   
   Allowed OPC
   Blocked OPC
   Allowed SIO
   Allowed DPC
   Blocked DPC
   STOP

   **Remarks:**
   
   A Link Set Group Identifier may be null, or a number between 1 and 99. Its use is described under the Allowed Calling Party Address table.

2. **Allowed OPC**

   **Provisioned Data:**
   
   An entry specifies a Network Identifier (NI), Network Cluster (NC), and Network Cluster Member (NCM). A range (e.g., 217-235) or a ‘wildcard’ indicator for the entire allowed range may be entered for NI, NC, or NCM.

   **Possible Next Steps:**
   
   Blocked OPC
   Allowed SIO
   Allowed DPC
   Blocked DPC
   Allowed CgPA
   STOP
   IGNORE

   **Remarks:**
   
   This screening table specifies all OPCs from which the STP is allowed to receive SS7 messages over a particular link set.
Allowed CgPA may be indicated as a next step if an STP performs SCCP screening after MTP screening was performed at another gateway STP.

3. **Blocked OPC**

   **Provisioned Data:**

   One entry specifies the next screening step only and is referred to when a matching entry is not found. The remaining entries specify a Network Identifier (NI), Network Cluster (NC), and Network Cluster Member (NCM). A range (e.g., 217-235) or a ‘wildcard’ indicator for the entire allowed range may be entered for NC, or NCM.

   **Possible Next Steps:**

   FAIL for an entry containing screening data

   For the one entry that indicates the next screening step if there are no matches:

   - Allowed SIO
   - Allowed DPC
   - Blocked DPC
   - Allowed CgPA
   - STOP

   **Remarks:**

   This table allows blocking of a set of OPCs. In particular, it allows blocking of a subset of allowed OPCs specified in the Allowed OPC table.

   Allowed CgPA may be indicated as a next step if an STP performs SCCP screening after MTP screening was performed at another gateway STP.

4. **Allowed Service Information Octet (SIO)**

   **Provisioned Data:**

   Service Indicator (SI)
   Network Indicator Code (NIC)
   Congestion priority (PRI)
   Heading codes H0 and H1 [for MTP network management and testing messages (Signaling Link Test and Acknowledgment)]

   A range or a single number are allowed for SI and PRI. A ‘wildcard’ indicator for the entire allowed range is allowed for NIC, PRI, H0 and H1.

   **Possible Next Steps:**

   - Allowed DPC
   - Blocked DPC
   - Affected Destination (may be provisioned for SI=0)
   - Allowed CgPA (may be provisioned for SI=3)
   - Allowed CdPA (may be provisioned for SI=3)
Allowed ISDNUP Message Type (may be provisioned for SI=5)
STOP
IGNORE

Remarks:
H0 and H1 values can be provisioned only when appropriate, i.e., for SI equal to 0, 1, or 2. Refer to GR-246-CORE, Issue 2, Chapter T1.111.4, Section 15 for a complete list of heading codes.
The NIC specifies a message formatting standard (national or international). GR-246-CORE, Issue 2, Chapter T1.111.4, Section 14 includes a description of the possible NIC codes.

5. **Allowed DPC**

*Provisioned Data:*
An entry specifies a Network Identifier (NI), Network Cluster (NC), and Network Cluster Member (NCM). A range (e.g., 217-235) or a 'wildcard' indicator for the entire allowed range may be entered for NI, NC, or NCM.

*Possible Next Steps:*
Blocked DPC
Affected Destination
Allowed CgPA
Allowed ISDNUP Message Type
STOP
IGNORE

Remarks:
This screening table specifies all DPC’s allowed to receive SS7 messages on the incoming link set.

6. **Blocked DPC**

*Provisioned Data:*
One entry specifies the next screening step only and is referred to when a matching entry is not found. The remaining entries specify a Network Identifier (NI), Network Cluster (NC), and Network Cluster Member (NCM). A range (e.g., 217-235) or a 'wildcard' indicator for the entire allowed range may be entered for NC, or NCM.

*Possible Next Steps:*
FAIL for an entry containing screening data
For the one entry that indicates the next screening step if there are no matches:
Affected Destination
Allowed CgPA
Allowed ISDNUP Message Type
STOP

Remarks:
This table allows blocking of a set of DPCs. In particular, it allows blocking of a subset of allowed DPCs specified in the Allowed DPC table.

7. **Affected Destination Field**

*Purpose:*
This screening step allows the STP to check that the affected destination in TFx/TCx, TFC, and signaling-route-set-test messages is allowed.

*Provisioned Data:*
An entry specifies a Network Identifier (NI), Network Cluster (NC), and Network Cluster Member (NCM). A range (e.g., 217-235) or a “wildcard” indicator for the entire allowed range may be entered for NI, NC, or NCM.

*Possible Next Step:*
STOP
IGNORE

Remarks:
A signaling-route-set-congestion-test message does not contain an affected destination field and hence this table is not applicable to it.

---

### C.3.2 SCCP Screening Tables

The flow of SCCP gateway screening is depicted in Figure C-3. Entry points at the top of this Figure feed from the corresponding exit points on the right of Figure C-2.

1. **Allowed Calling Party Address (CgPA)**

*Provisioned Data:*

CgPA PC
It consists of a Network Identifier (NI), Network Cluster (NC), and Network Cluster Member (NCM). A range (e.g., 217-235) or a “wildcard” indicator for the entire allowed range may be entered for NI, NC, or NCM. This parameter may be absent (e.g., in the case of a CLASS query). If a global title translation is indicated in the Calling Party Address, the Calling Party Address will contain an SSN, a translation type of 4 (Global Title = PC), and a global title consisting of the point code. Screening shall proceed as before.
CgPA SSN
Link Set Group Identifier
Called Party Address (CdPA) Routing Indicator (RI) (note that the RI is from the CdPA, contrary to the name of the screening table)
SCCP Message Type (UDT, XUDT, UDTS, XUDTS)

A range may be entered for SSN. A “wildcard” indicator for the entire allowed range may be entered for RI, SSN, or Link Set Group Identifier. Link Set Group Identifier parameter is optional.

Possible Next Steps:
Allowed TT (may be provisioned if RI=0)
Allowed CdPA (may be provisioned if RI=1)
STOP
IGNORE

Remarks:
The Link Set Group Identifier parameter (see Gateway Link Set table description) is included to allow a network administrator to specify the same MTP screening but different SCCP screening for several groups of link sets.

The screened RI is the original parameter value in the received message, not the RI derived after global title translation.

The motivation for including the SCCP Message Type is described in Section C.4.

2. **Allowed Translation Type (TT)**

   Provisioned Data:
   Translation Type
   A range may be entered.

   Possible Next Steps:
   Allowed CdPA
   STOP
   IGNORE

   Remarks:
   Messages screened during this step have a CdPA Routing Indicator (RI) of 0 and therefore require SCCP routing.
3. **Allowed Called Party Address (CdPA)**

   *Provisioned Data:*
   
   Routing Label DPC
   It consists of a Network Identifier (NI), Network Cluster (NC), and Network Cluster Member (NCM). A range (e.g., 217-235) or a “wildcard” indicator for the entire allowed range may be entered for NI, NC, or NCM.
   
   CdPA SSN
   SCMG (SCCP Management) Format ID (may be provisioned if SSN=1)

   *Possible Next Steps:*
   
   Affected Point Code/Subsystem Number (may be provisioned if SSN=1)
   STOP
   IGNORE

   *Remarks:*
   
   If GTT is required, it should be performed prior to this screening step.

4. **Affected Point Code and Subsystem Number (PC/SSN)**

   *Purpose:*
   
   This screening step allows the STP to check that the affected PC and SSN in SCCP management messages (CdPA SSN=1) are allowed.

   *Provisioned Data:*
   
   Affected PC
   It consists of a Network Identifier (NI), Network Cluster (NC), and Network Cluster Member (NCM). A range (e.g., 217-235) or a “wildcard” indicator for the entire allowed range may be entered for NI, NC, or NCM.
   
   Affected SSN
   A range or a “wildcard” indicator for the entire allowed range may be entered for SSN.

   *Possible Next Steps:*
   
   STOP
   IGNORE

**C.3.3 ISDNUP Screening Table**

1. **Allowed ISDNUP Message Type**

   *Provisioned Data:*
   
   ISDNUP Message Type (e.g., IAM, ACM, CGB, etc.)
Possible Next Steps:

STOP
IGNORE

Remarks:

See Section C.4.

C.4 Motivation for New Screening Requirements

This subsection discusses the motivation for new gateway screening requirements that appeared for the first time in TA-NWT-000082, Issue 6. The new requirements are:

— Inclusion of the SCCP Message Type parameter in the Allowed CgPA gateway screening table
— ISDNUP Message Type screening
— Gateway Message Rejection Reporting Suppression.

C.4.1 SCCP Message Type Screening

When an SCCP message from the Bcc network is sent to another network by means of SCCP routing and an STP performing SCCP routing in a foreign network is unable to forward the message for some reason (e.g., no translation for the specified Global Title Address), that STP will send an (X)UDTS message to the CgPA in the original (X)UDT message. The CgPA in the (X)UDTS message will be the Called Party Address (CdPA) in the original (X)UDT message since the STP sending the (X)UDTS message essentially swaps the Calling and Called Party Addresses from the (X)UDT message. Thus, the CgPA in the (X)UDTS message may contain the Global Title and SSN, rather than the usual PC and SSN in an (X)UDT message. Hence, a different CgPA screening may need to be applied to (X)UDTS messages compared to (X)UDT messages. The inclusion of the SCCP Message Type parameter in the Allowed CgPA screening table will allow an STP to apply different screening. (Note that the OPCs in (X)UDTS messages may differ from the OPCs in the (X)UDT messages.)

C.4.2 ISDNUP Message Type Screening

The motivation for including ISDNUP screening based on ISDNUP Message Type is that such screening will permit a Bcc to accept ISDNUP messages only of appropriate congestion priority, e.g., 0 or 1 for IAM, 1 for ACM, 2 for ANM, etc. To perform ISDNUP screening based on congestion priority, appropriate provisioning of the Allowed SIO table must be performed by the network administrator. In addition, such ISDNUP screening may
be used to reject ISDNUP messages that remove switch resources from service or to reject ISDNUP messages with undefined or unimplemented Message Types.

C.4.3 Gateway Message Rejection Reporting Suppression

In addition, a new capability has been added to allow a user to specify that certain messages should be failed (rejected) and not reported. This will be achieved through the use of the existing screening tables. The method that will be used to accomplish this is to allow a new Next Step with the value IGNORE. This will indicate for the STP to reject the message, and not report it to the SEAS System. The STP should, however, continue to include these message rejections in the measurements defined in Section C.6. An example of how this would be used is that sometimes a CCS Network will get unwanted TFx/TCx messages regarding nodes that the CCS Network does not route to and has no interest in. These messages will get screened out (rejected), but will also get reported to the user. However, since the user has no business interest in investigating these rejection reports, they don’t want them reported. The users of the SEAS System have expressed interest in a general way to specify which messages are not to be reported.

C.5 Gateway Screening Requirements

RC-1 An STP shall have the ability to implement the MTP, SCCP, and ISDNUP screening functions according to the gateway screening tables described in Sections C.3.1, C.3.2, and C.3.3.

RC-2 Gateway screening tables shall be provisionable via the SEAS system interface and local craft interface.

Provisioning of gateway screening tables via the SEAS system interface is described in detail in GR-778-CORE. GR-778-CORE also states additional requirements on validations of input parameters and parameter relationships, reporting of screening rejections, and data collection.

RC-3 An STP shall conform to additional gateway function requirements in GR-778-CORE.

RC-4 is necessary to allow a smooth transition to the ISDNUP Message Type screening capability and the introduction of the SCCP Message Type parameter into the Allowed CgPA screening table.

RC-4 Introduction of the ISDNUP Message Type screening capability into the screening tables shall not require manual reprovisioning of data already provisioned in the screening tables for other screening steps. Likewise, introduction of the SCCP Message Type screening capability
into the Allowed CgPA screening table shall not require manual reprovisioning of data already provisioned in the screening tables for other screening steps.

By way of clarification, the preceding requirement may be interpreted as follows. Upon installation, the new screening tables and software shall be transparent to the functioning of currently working screening capabilities. That is, the new gateway screening package shall be initialized to conduct gateway screening according to procedures currently used. Phrased in another way, there shall be no need for the network administrator(s) to repopulate the gateway screening tables with already provisioned and operational data just to continue screening as it is currently conducted.

Two additional requirements in the area of reporting message screening rejections to the SEAS system are considered below.

As discussed in GR-778-CORE, an STP must be capable of throttling back reports of message screening rejections. The throttling mechanism shall be such that an STP reports the first “n” rejections (unique or not) every “m” minutes, m and n being provisionable. An additional capability is provided for the first time to throttle back rejection reports of certain user-specified messages. The user specifies which rejections should not be reported by putting “IGNORE” as the next step (in all but the gateway link set and the blocked tables), as was indicated in Sections C.3.1 through C.3.3 and as illustrated in Figure C-2 and Figure C-3.

When the STP does not report rejections of messages, it should still count them in the measurements of rejected messages.

Currently, when an STP reports to SEAS a message screening rejection, it does not include in the report the contents of the rejected message. It is desirable that an STP provide a capability to include the entire rejected message because such information may be helpful in troubleshooting. This capability is discussed in the next requirement.

**RC-5** [473] An STP shall provide a provisionable ON/OFF switch for including the entire SS7 message in a message rejection report to SEAS. When the switch is provisioned ON, the entire message shall be included, and when the switch is provisioned OFF, the message shall not be included.

### C.6 Measurements

The following additional measurements are specific to a gateway STP or an STP performing gateway screening.
C.6.1 System Totals

RC-6 [474] An STP performing gateway screening shall maintain the following system total 30-minute measurements for each interconnecting CCS network (ICN). An ICN is another signaling network that has a direct or indirect signaling link connection to a Bcc CCS network. Because the other network may not be directly connected by signaling links, but may access the Bcc CCS network via an intermediate network, these measurements shall be maintained per network identification (Network Identifier subfield or Network and Cluster Identifier subfields for small networks) of the OPC in the messages.

… A. Number of global title translations performed on messages received from the interconnecting network by translation type.

… B. Number of global title translations that cannot be performed on messages received from the interconnecting network because of no translation table for this translation type.

… C. Number of global title translations that cannot be performed on messages received from the interconnecting network because of no translation for this address by translation type.

… D. Number of global title translations performed that result in a DPC in the interconnecting network.

C.6.2 Link Set Utilization

RC-7 [475] A gateway STP shall maintain the following 30-minute measurements on a per-link-set basis for the internetwork link sets listed in the Gateway Link Set table. Where counts are defined by originating network or by terminating network, a separate measurement shall be kept for each originating or destination network. These measurements shall only include valid messages that have passed the initial screening.

… A. Number of message signal units (MSUs) received from another network that are not addressed to the Bcc network, by destination network.

… B. Number of MSU octets received from another network that are not addressed to the Bcc network, by destination network.

… C. Number of MSUs transmitted that are addressed to a network other than the adjacent receiving network, by destination network.

… D. Number of MSU octets transmitted that are addressed to a network other than the adjacent receiving network, by destination network.
E. Number of transfer-prohibited and transfer-cluster-prohibited messages transmitted/received (two separate measurements, one for each direction, each measurement covers TFP and TCP messages).

F. Number of transfer-restricted and transfer-cluster-restricted messages transmitted/received (two separate measurements, one for each direction, each measurement covers TFR and TCR messages).

G. Number of transfer-allowed and transfer-cluster-allowed messages transmitted/received (two separate measurements, one for each direction, each measurement covers TFA and TCA messages).

H. Number of signaling-route-set-test and signaling-route-set-cluster-test messages transmitted/received (two separate measurements, one for each direction, each measurement covers signaling-route-set-test and signaling-route-set-cluster-test messages).

I. Number of transfer-controlled messages received by the Gateway STP, by originating network.

J. Number of transfer-controlled messages transmitted by the Gateway STP, by destination network.

K. Number of signaling link test messages received.

L. Number of signaling-route-set-congestion-test messages transmitted/received (two separate measurements, one for each direction).

M. Number of testing and maintenance messages received.

N. Number of subsystem-prohibited (SSP) messages transmitted/received (two separate measurements, one for each direction).

O. Number of subsystem-allowed (SSA) messages transmitted/received (two separate measurements, one for each direction).

P. Number of subsystem-status-test (SST) messages transmitted/received (two separate measurements, one for each direction).

**C.6.3 Screening Results Measurements**

**RC-8**  [476] An STP performing gateway screening shall maintain the following 30-minute measurements on a per-link-set basis. Totals for number of MSUs rejected due to failure of screening, by originating network and by cause for screening failure shall be kept for

1. Invalid OPC
2. Invalid DPC
3. Invalid SI
4. Invalid NIC
5. Invalid PRI
6. Invalid H0 or H1
7. Invalid affected destination field in network management message, by message type (as defined by H0 and H1 codes)
8. Testing and maintenance messages incorrectly addressed to other than the Gateway STP
9. Invalid SCCP CgPA (PC/SSN)
10. Invalid affected PC in SCCP SSP and SSA messages
11. Invalid affected PC/SSN in SCCP subsystem status test (SST) messages
12. Disallowed SCCP CdPA (PC/SSN) by Calling Party Address, DPC/SSN
13. Disallowed DPC/SSN as a result of global title translation, by Calling Party Address, by resultant DPC/SSN
14. Disallowed Translation Type (TT), by TT
15. Disallowed ISDNUP message type, by message type.

OC-9 [564] When determining which error code to attribute a message failure for SIO, CGPA, and CDPA screening, the Objective (O6-11 [94]) in GR-778-CORE shall be followed.

C.6.4 Maintenance Measurements

RC-10 [477] A gateway STP shall provide an additional measurement in the system performance category (this category is considered in Section 6.4.2). This measurement shall consist of (daily, hourly) counts of the number of MSUs discarded due to screening. A separate count shall be kept for each signaling link set, by originating network.

C.7 Performance

Section 8.2 describes the STP performance requirements for STP transport time, including gateway screening.
RC-11 [478] Gateway screening shall not affect the STP node processing time beyond the requirements that Section 8.2 presents.

Figure C-1. Interaction among Functionalities of MTP and SCCP Processing and Gateway Screening
Fig. C-2. Possible Flow of MTP Screening Steps

* The terms “Blocked OPC” and “Blocked DPC” are defined in Section C.2.1.
Figure C-3. Possible Flow of Screening Steps for MTP Network Management Messages, SCCP, SCCP Management, and ISDNUP Messages
Appendix D: Cluster Routing and Management at STPs

This appendix describes Bellcore’s view of the procedures that apply when STPs perform cluster routing and management. It includes background material and presents a complete view of the cluster routing and management model. Section 4.2 defines specific, verifiable requirements for cluster routing and management. The information this appendix describes is not intended to constrain any acceptable implementation. It is intended to serve as a data model that can be used to describe externally visible STP behavior. This appendix is included as general explanatory information and does not contain any requirements.

D.1 Introduction

In Appendix D, a cluster is defined to be a group of signaling points that are identical in the Network ID and Network Cluster fields of their point codes. The term route is used to mean a link set used to transmit messages toward a given destination. It implies an association between a link set and a destination, since a single link set may be associated with multiple routes to different destinations. A normal route is a route that an STP would select to transmit a message toward a given destination, under normal (non-failure) conditions. An alternate route is a route that an STP would select to transmit a message toward a given destination if no normal routes could be used. If multiple alternate routes are discussed, they are referred to as the first and second alternate route, where the first alternate route is of higher priority than the second alternate route. A route set is the term used to mean the collection of normal and alternate routes that may be used to route messages toward a given destination.

A destination is a generic term that refers to either a cluster or a member. If a route set is provisioned with the destination being a cluster, it is considered a cluster route set, and the routes within the route set are considered cluster routes. If a route set is provisioned with the destination being a member, it is considered a member route set, and the routes within the route set are considered member routes. A route within a route set is provisioned with the following pieces of information: the destination, the link set, and the cost or priority of the route. The current route status is also maintained (on a dynamic basis) for each route in a route set.

When determining a route over which a message should be sent, a node may use the full 24-bit Destination Point Code (DPC), examining the Network ID, Network Cluster, and Cluster Member fields, or it may use only the Network ID and Network Cluster portions of the DPC to determine the proper outgoing route. In the former case, the node consults a member route set, and is performing full point code or member routing; in the latter case, the node consults a cluster route set, and is performing cluster routing. Cluster routing and management refer to procedures that use partial point code information (i.e., the Network ID and Network Cluster fields of the DPC present in each SS7 message) to route MSUs and perform network management functions, as well as procedures that determine how to respond to signaling route management messages that refer to clusters (i.e., transfer-cluster-
prohibited [TCP], transfer-cluster-restricted [TCR], transfer-cluster-allowed [TCA],
signaling-route-set-cluster prohibited [RCP], and signaling-route-set-cluster restricted
[RCR] messages) or members (i.e., transfer-prohibited [TFP], transfer-restricted [TFR],
transfer-allowed [TFA], signaling-route-set prohibited [RSP], and signaling-route-set
restricted [RSR] messages). Even if a destination is provisioned as a cluster, the node must
still respond to TFP, TFR, and TFA (i.e., TFx) messages and RSR and RSP (i.e., RSx)
messages, and if a destination is provisioned as a member, the node must still respond to
TCP, TCR, and TCA (i.e., TCx) messages and RCR and RCP (i.e., RCx) messages.

Some of the functions described in this section rely on two fundamental capabilities being
present in an STP:

1. The STP should be able to broadcast TFx messages to all adjacent nodes, even if the
   only available route to the adjacent node is non-direct.

2. The STP should maintain two statuses for each route. First, it should maintain
   information regarding whether the link set corresponding to the route is “available” or
   “unavailable.” Second, it should maintain information regarding the routing status for
each node or cluster accessible via that route (i.e., for each point code or cluster, which
TFx or TCx message was last received). These two statuses are independent from one
another, and are described further in Section D.3, Status Definitions.

D.1.1 Cluster Routing and Management Diversity (CRMD)

The model of cluster routing and management presented in this appendix includes new
material that, collectively, is referred to as cluster routing and management diversity
(CRMD). This material provides a mechanism that allows both cluster and member routes
to be provisioned in the same cluster. The CRMD model provides more flexibility over the
cluster routing and management (CRM) model in terms of route management. (The CRM
model was discussed in previous issues of TR-NWT-000082. See also Section 4.2.4.11.)
For example, it allows E-links to be deployed to a remote cluster, and still supports cluster
routing to be provisioned for those cluster members that are not connected via E-links. On
the other hand, when the CRM model is used at an STP and E-links are deployed from the
STP to a member of a remote cluster, then the STP must perform member routing for every
member of the cluster, even if the E-links are only deployed to a single cluster member.
This consequence is due to the fact that an E-link deployed to a member of a remote cluster
gave the STP direct connectivity to that cluster.

In the CRMD model, member route sets and cluster route sets are considered associated if
they are administered in the same cluster (i.e., if the point codes of the destinations are
identical in the Network ID and Network Cluster fields). This concept is in contrast to
previous versions of this GR that assumed that only cluster or member routes could be
provisioned in a cluster, but not both. In this new model, the following assumptions are
made with regard to the administration and consultation of route sets:
• one cluster route set can be provisioned for a cluster
• one member route set can be provisioned for any cluster member
• when determining a route over which an MSU should be sent, the STP consults a member route set, if one is provisioned for the DPC in the message. If no member route set is provisioned, it consults the cluster route set.

D.2 Applicability of Cluster Management

A cluster route set may only be provisioned if all members that use the route set share the same routing from the STP, as described in Section 13.2.2A of T1.111.4 of GR-246-CORE. That is, the normal route, and all alternate routes are the same for each member of the cluster. This typically occurs when a node is not directly connected to a member, such as when an STP must route all messages toward a cluster through another STP. On the other hand, when cluster routing and management diversity is used, a member route set must be provisioned if a member can be reached via at least one route that is different from the other members of the cluster. This typically occurs when the node is directly connected to the member, such as when an STP has A-links or E-links connected to a member.

Examples are presented in the following paragraphs.

Consider the network configuration shown in Figure D-1 (located at the end of this appendix). Two types of clusters are defined, local and remote.

From STP 1’s point of view, cluster L (consisting of members a, b, and c) is a local cluster. All the members are directly adjacent to STP 1, and no intermediate STPs are required to route to those particular point codes. Consequently, each member of a local cluster requires a different route set, therefore a member route set must be provisioned for each member. For example, STP 1’s routing table for member a might show LS1 as the normal route, whereas for member b, LS2 would be the normal route.

From STP 1’s point of view, cluster R (consisting of members x, y, and z) is a remote cluster, since none of cluster R’s members are adjacent to STP 1. In this situation, STP 1 must use another mated pair of STPs as intermediate nodes, when routing messages to any node within cluster R. This scenario illustrates that it is sufficient to provision only one cluster route set for a remote cluster, since the routing is identical for each member. In this case, the route set for cluster R would most likely show LS4 and LS5 as the normal routes, and the C-link set as the alternate.

Cluster routing is most appropriate for remote clusters. However, the fact that cluster routing is appropriate for remote clusters does not mean that it must be used for remote clusters. It is acceptable, in the provisioning process, for a remote cluster to be administered with full point code (i.e., member) routing. In that case, it is still necessary for the STP to understand and appropriately act on received cluster network management messages (i.e., TCx messages) pertaining to that cluster, just as it is necessary for the STP to understand
and appropriately act on member network management messages (i.e., TFx messages) that affect signaling points administered on a cluster basis.

D.3 Status Definitions

The definitions pertaining to signaling link status, signaling status, and overall routing status are as described in Sections 4.2.4.11.1, 4.2.4.11.2, and 4.2.4.11.3, respectively. These definitions are intended to reflect the existing cluster management messages defined in GR-246-CORE.

D.4 Cluster Status Maintenance

The distinction between a local and remote cluster is that a local cluster is directly adjacent to an STP, whereas a remote cluster is only reachable through other STPs. For a local cluster, member routing is necessary, and for a remote cluster, the STP may perform cluster or member routing.

However, being unable to maintain the status of individual point codes when a node is performing cluster routing can lead to some potentially serious situations involving message loss, congestion, and reduced network efficiency. To illustrate this point, assume (in Figure D-1) that links 1 and 4 fail, and that STP 1 only maintains a cluster status on each cluster route for remote cluster $R$. Under these circumstances, STP A would send a TFP for member $x$ of cluster $R$ to STP 1. However, STP 1 has no routing table entries for the individual members of cluster $R$, so it discards the TFP from STP A and does not change its routing. STP 1 then continues to route MSUs via STP A destined to $x$. These messages would be discarded by STP A.

To avoid the above scenario and others like it, STPs should be able to maintain the routing status of individual cluster members which have a more restrictive status than the cluster on a given cluster route. They do this by maintaining a dynamic routing exception list (referred to as an “x-list”) for tracking the status of individual cluster members. An x-list, as used in this document, refers to a list of individual cluster members which have a more restrictive status than that of the cluster to which they belong, for a given cluster route. Thus, the cluster status on a cluster route represents the routing status of the least restrictive cluster member on the route, and the x-list contains the members that do not conform to that status. The x-list is dynamic, in the sense that its size changes as members are placed on it and removed from it. Separate x-lists should be maintained for a given cluster for each route in a cluster route set, just as, for full point code routing, a separate status is maintained for each route in a member route set. An x-list is maintained for each cluster route to keep the status of the more restrictive members of the cluster on the cluster route separately from the cluster status on the same route and when cluster routing and management diversity is used, an x-list is not used to store routing information of a member for which member route set is provisioned. An x-list for a cluster allows an STP to dynamically record the change in
the status of cluster members on a cluster route so that appropriate message routing and
network management functions for those members can be performed.

When an STP needs to route a message to a member of a cluster, it should first determine
if a member route set is provisioned for the point code to which the message is destined. If
it is, it should consult that member route set to determine a route over which to send the
message. To determine whether a particular route may be used, it should check the status
of the member on the route. If a signaling route to a member destination is unavailable, no
messages for the destination should be sent over the route. If a signaling route to a member
destination is restricted, the STP should avoid sending messages over that route, if possible.
If a signaling route to a member destination is available, then the STP may send messages
over that route.

If a member route set is not provisioned for the point code to which the message is destined,
and a cluster route set is provisioned for the cluster of which the point code is a member, it
should consult the cluster route set to determine a route over which to send the message. To
determine whether a particular route may be used, it should check the cluster status for
applicable routes in the route set. Note that the following rules only apply if a member route
set is not provisioned:

• If a cluster route is unavailable, then no messages for any destination in the cluster
  should be sent over that route.

• If a cluster route is restricted and the particular destination is not marked as prohibited
  on the cluster’s x-list for the route, the STP should avoid sending messages over that
  route, if possible.

• If a cluster route is available and the particular destination is marked neither prohibited
  nor restricted on the cluster’s x-list for the route, the STP may send messages over that
  route.

• If a destination is marked as restricted on a cluster’s x-list for a route the STP should
  avoid sending messages to that destination over that route, if possible.

• If a destination is marked as prohibited on a cluster’s x-list for a route, no messages
  for the destination should be sent over that route.

The general rules for modifying x-lists follow:

• An x-list only maintains the status of a point code. When cluster routing and
  management diversity is used, the status of a point code is maintained on an x-list if a
  member route set is not provisioned for that point code.

• Point codes are placed on a cluster’s x-list if a TFR or TFP message is received and
  the cluster route status is less or, as a supplier option, equally restrictive.

• Point codes are individually removed from a cluster’s x-list if a TFA or TFR message
  is received, indicating a point code status the same as the status of the cluster to which
  the affected point code belongs. (As a supplier option, when a TFR is received for an
SP and the SP is marked prohibited on the x-list, the route status of the SP may be updated to restricted and kept on the x-list as long as the cluster is marked restricted on that route.)

• The status of a point code marked prohibited on a cluster’s x-list is changed to restricted upon receipt of a TFR message referring to the affected point code.

• All point codes marked restricted on an x-list may be removed upon receipt of a TCR message. Alternatively, they may be left on the x-list. This choice is a supplier option.

• All point codes marked restricted on an x-list are either removed or changed to prohibited, if a TCP message is received referring to the cluster of which the point code is a member. This choice is a supplier option.

• All point codes marked prohibited on an x-list may be removed if a TCP message is received referring to the cluster of which the point code is a member. Alternatively, they may be left on the x-list. This choice is a supplier option.

To illustrate some of the above rules, consider Figure D-1. If the cluster R is marked allowed on a given cluster route, STP 1’s x-list might contain point codes marked restricted or prohibited. If a TCP message is received about the cluster, all point codes on the x-list may be removed. If the cluster is marked allowed on a given cluster route, and a TCR message is received, only point codes marked as restricted in the x-list may be removed. Point codes marked as prohibited in the x-list should be retained because these point codes are maintained whenever the corresponding cluster is marked allowed or restricted on that cluster route.

A point code on an x-list is also removed if it remains on the x-list for a considerable period of time without a change in its status, and if no traffic addressed to that point code arrived at the STP while the timer is running. If the timer expires, and traffic addressed to the point code has arrived at the STP while the timer was running, the timer is restarted. The length of time should be administrable, with a suggested range between 20 minutes and 24 hours.

If, in the example above, STP 1 maintained x-lists for cluster R, the following events would occur. When links 1 and 4 fail, STP A would send a TFP message for point code x to STP 1. Upon receipt of the TFP message, STP 1 would add point code x to its x-list, mark it prohibited on route LS4. (The cluster route status is not changed.) The STP would then route any subsequent messages for this point code via another route (e.g., LS 5), even though traffic for the rest of cluster R would continue to be sent on LS4. If link 1 were then restored, STP A would send a TFA for point code x to STP 1. At that point, STP 1 would remove x from the x-list, and reestablish normal routing for x.

The conditions under which x-lists should and should not be maintained for cluster routes at an STP follow:

• When a remote cluster is marked as prohibited on a particular route. This implies that no member of the cluster that uses the cluster route set may be reached via that route. Therefore, it is not necessary to maintain an x-list for a cluster which is marked
prohibited on a route. As a supplier option, however, the STP could maintain members marked prohibited on the x-list.

- When a remote cluster is marked as restricted on a particular route, the STP should avoid using the route, if possible, for any member of the cluster that uses the cluster route set. In this situation, it is possible that there are members for which the STP should never use the route, because those members are marked prohibited on the route. This could occur due to failure of A-links. Therefore, it is necessary, for a cluster which is restricted on a route, to maintain an x-list of members which are marked prohibited on that route. As a supplier option, the STP could also maintain members marked restricted.

- When a remote cluster is marked allowed on a particular route, the cluster route may be used, without restriction, for all members of the cluster that uses the cluster route set. In this situation, it is possible that one or more members of the cluster are marked restricted or prohibited. Therefore, it is necessary, for a cluster which is marked allowed on a route, to maintain an x-list of members which are marked restricted or prohibited on that route.

As implied previously, one of the motivations for administering cluster routing toward a particular cluster is that it reduces the static memory requirements required to store the route status for that cluster. However, additional memory is still needed to store the route status for members on the x-list for the cluster on a route. It is a goal to minimize the amount of additional x-list memory needed. Recognizing that the precise sizing of this x-list memory is closely tied to product architecture, the following general concerns should be considered by any supplier implementing cluster management in their product.

- The way a product allocates x-list memory (e.g., the number of members that may be stored in a block of memory and the mechanism for determining which cluster gains access to a block of memory) should be designed to ensure that memory will be available to store the status of an x-list member, when needed.

- The location of a node in the architectural hierarchy of a network has an impact on the expected number of TFx messages that could be received about individual cluster members, which, in turn, has an impact on the amount of x-list memory needed. For example, as the number of STP hops to a particular cluster increases, the likelihood that a TFx message will be received about a member of the cluster decreases (though not necessarily in direct proportion), so it is likely that less entries would be placed on an x-list for a cluster on a route. Therefore the required x-list memory at a node that is a single STP hop away from a cluster is greater than the memory required if the same node is several STP hops away from the cluster. The precise amount of memory needed is therefore dependent not only on product design, but also on the network topology.

- The expected or average number of members in a cluster may vary from one network to another, so the maximum number of members that could be on an x-list in a given network may vary from one network to another.
The above considerations are not intended to be an exhaustive list of concerns; they are intended to point out the criticality of x-list sizing, and some issues to consider when designing an implementation of cluster management.

Even if x-lists are sized appropriately, maintaining an x-list for a cluster on every cluster route still consumes STP resources. To provide Bccs with a mechanism for tuning the resources used at the STP, they should be able, when administering a cluster route set, to determine whether or not the STP should maintain x-lists for the cluster. Thus, if a Bcc determines that a particular cluster has a low community of interest with the STP, it should be able to administer the cluster routing information so that no x-list is maintained for the cluster, to free up resources for other STP functions. This might be useful for a remote cluster, toward which the STP does not transfer many messages. However, if this option is selected, a Bcc should be aware of the potential for message loss, toward members of remote clusters that are prohibited via the STP, but for which no x-list entry is made. The Bcc should also consider the consequences of such message loss.

There are situations that occur when an STP is performing cluster management, when the STP should broadcast certain network management messages. Specifically, when the STP determines that a cluster has become either inaccessible or accessible via normal route(s), it should broadcast TCP or TCA messages, respectively. In addition, when the STP determines that a particular member has become either inaccessible or accessible via normal route(s), the STP should broadcast TFP or TFA messages, respectively. To further provide a mechanism by which a Bcc can tune STP resource usage, it is desirable that a Bcc be able to administer whether or not the STP should broadcast these messages for particular clusters. Note that this mechanism only applies to the broadcast method of sending such messages; it does not affect the response mode method of sending the messages. Note, however, that if this option is selected for an inaccessible cluster or cluster member, then messages arriving at the STP from an adjacent node, destined for the remote cluster, would get lost until a response mode TCP or TFP message could be sent to the node. In addition, when the cluster or cluster member becomes accessible via normal route(s), selecting this option would delay conveying the cluster or member’s availability to adjacent nodes, until an RCP or RSP message is received from each node. Therefore, if the option is selected, then when an inaccessible cluster or cluster member becomes accessible via normal route(s), it could take up to 30 seconds to convey this status to adjacent nodes. Before selecting this provisioning option, a Bcc should consider the effects of delaying informing adjacent nodes when clusters or cluster members become inaccessible or accessible via normal route(s).

D.4.1 Additional Status Maintenance Rules for Cluster Routing and Management Diversity

The general rules for changing the status of routes in member route set(s), when an associated cluster route is administered are as follows:
• If a TFx message is received for a destination over a route contained in the destination’s member route set, the status of the member on the affected route is changed to match the status in the received message, if the cluster status on the associated cluster route is not equally restrictive as, or more restrictive than the status indicated in the received message.

• If a TCx message is received for a cluster over a route contained in an associated member route set, then the status of the member on the affected route should be changed to match the cluster status in the received message, if that status is more restrictive than the current member status.

To illustrate some of the above rules, consider Figure D-1, and assume that an E-link set is deployed from STP 1 to member \( x \) of cluster \( R \). This would require that a member route set be provisioned for member \( x \). The member route set could show the E-link as the normal route, links LS4 and LS5 as the first alternate routes, and the C-link set as the second alternate route. This member route set would be associated with the cluster route set for cluster \( R \). Now, if STP 1 received a TCR message over route LS4, it would mark the cluster \( R \) restricted on cluster route LS4, and it would mark member \( x \) on the associated member route LS4 as restricted. If a TFP message were then received for member \( x \) over route LS4, STP 1 would mark the member \( x \) as prohibited. If a TCA message were later received, STP 1 would mark the cluster \( R \) on cluster route LS4 as allowed, but it would not change the status of member \( x \) until it received a TFR or TFA message about the member.

D.5 Procedures for Cluster Management at STPs

This section describes the detailed procedures that an STP should perform in support of cluster management. As stated prior, this material is not intended to constrain any acceptable implementation; it is included to ensure a uniform view of the external behavior of the STP.

In the following sections, when an error condition is cited for a particular management message, it implies that the specific management message should not be received or sent if cluster routing and management procedures, described in this section, are fully implemented.

D.5.1 Full Point Code Management

Some actions related to cluster management interact with actions related to full point code management. The following section describes the actions that should be taken, if only member route sets are provisioned in a cluster.
D.5.1.1 Sending TFx and TCx Messages

The rules for transmission of TFx (i.e., TFP, TFR, and TFA) and TCx (i.e., TCP, TCR, and TCA) messages about clusters and cluster members for which only member route sets are provisioned are not changed by cluster management.

Consistent with the network option described in Section 13.2.2A of T1.111.4 in GR-246-CORE, TCx messages are generally only sent for a cluster if the same route set is used by the STP to route to every member of that cluster, as in the case when only a cluster route set is provisioned for a remote cluster. Therefore, it is not necessary for an STP to transmit TCx messages about a cluster for which only member route sets are provisioned. For example, in Figure D-1, STP 1 is not expected to send TCx messages to STP A for cluster L.

D.5.1.2 Receiving TFx and TCx Messages

The procedures the STP should perform when it receives a TFx message for a member of a cluster for which only member route sets are provisioned are not changed by cluster management.

Even when the STP only has member route sets provisioned for a particular cluster, it is possible for it to receive TCx messages from other nodes about that cluster. In the following cases, if the route over which the TCx message is received is not in a member route set used by the STP to route messages to a member of the affected cluster, the TCx message should be ignored. Otherwise, the following actions should be taken:

- TCP Received:
  When an STP receives a TCP message from an adjacent node about a cluster for which it only has member route sets, the originator of the message has started using the STP as its route for the cluster. Therefore, upon receipt of the TCP message, the STP should mark any members for which a member route set is provisioned as prohibited on that route.

- TCR Received:
  When an STP receives a TCR message from an adjacent node about a cluster for which it only has member route sets, the STP should mark any members for which a member route set is provisioned as restricted on that route.

- TCA Received:
  When an STP receives a TCA message from an adjacent node about a cluster for which it only has member route sets, the STP should mark any members for which a member route set is provisioned as allowed on that route.
D.5.1.3 Sending RSx and RCx Messages

The rules regarding when to initiate RSx (i.e., route-set-test-restricted [RSR] and route-set-test-prohibited [RSP]) messages for members of a cluster for which only member route sets are provisioned are not changed by cluster management, but some additional criteria regarding when to stop sending the RSx messages are needed. The basis for these criteria is an assumption that, if only member route sets are provisioned in a cluster, no cluster status is maintained for a route. Therefore, any received TCx message would affect every individual cluster member, and would not simply change the cluster status. These criteria follow:

• Stopping Transmission of RSR and RSP messages

If RSR or RSP messages are being sent about a member of a cluster for which only member route sets are provisioned, and a TCx message about the cluster is received over the affected route, the STP should stop sending the RSR and RSP messages. If a TCR or TCP message is received, the STP should proceed with the steps listed below.

Under certain conditions, TCx messages may be received by the STP for clusters which only have member route sets provisioned (For example, when the network configuration shown in Figure D.2 is deployed and the RSTP pair does full PC routing to cluster L and the LSTP 1 pair does cluster routing to cluster L, LSTP 1 pair may send TCx messages to the RSTP pair if the status of cluster L from the LSTP 1’s perspective changes). However, for the situations described in Section D.5.1.2, when a TCx message is received, the following actions should be taken, if the route over which the TCx is received is in the member route sets that the STP uses to route messages to the members of the cluster.

• TCP Received

If a TCP message is received, the STP, should begin sending route-set-cluster-prohibited (RCP) test messages for the affected cluster to the originator of the TCP message, every T1.111.4/T10 seconds, until it receives a TCR or TCA message for the affected cluster from the originator of the original TCP message. Optionally, it is acceptable, but not preferred, for the STP to send individual route-set-prohibited (RSP) test messages for all members of the affected cluster, instead of RCP test messages for the cluster.

• TCR Received

If a TCR message is received, the STP should begin sending route-set-cluster-restricted (RCR) test messages for the affected cluster to the originator of the TCR, every T1.111.4/T10 seconds, until it receives a TCP or TCA message for the affected cluster from the originator of the original TCR message. Optionally, it is acceptable, but not preferred, for the STP to send individual route-set-restricted (RSR) test messages for all members of the affected cluster, instead of RCR test messages for the cluster.
D.5.1.4 Receiving RSx and RCx Messages

The rules for receiving and responding to RSx messages for a member of a cluster for which only member route sets are provisioned are not changed by cluster management.

Receipt of an RCx message by an STP for such a cluster is an error condition, if a corresponding TCx message is not initially sent from the STP. However, to minimize problems that could result from such a received message, the STP should reply to that message with a TCA message, if it only has member route sets provisioned in the affected cluster.

D.5.1.5 Actions Taken by the STP Upon Receipt of a TFx or TCx Message

Table D-1 specifies the actions the STP should take for a member of the cluster, upon receipt of TFx and TCx messages, when only member route sets are provisioned in a cluster. Signaling point \( z \) refers to the member for which a member route set is provisioned, and \( R \) refers to the cluster to which the member belongs. All table entries that have a dash (-) are either considered error conditions or conditions where no action for member \( z \) should be taken by the STP. For table entries indicating a route (member) status change from a more restrictive to a less restrictive status, rerouting (i.e., controlled) is performed when the route with status change is of higher priority than or equal priority to the one which is currently used for the destination or in some cases when the route status change is for the current route.

<table>
<thead>
<tr>
<th>Member ( z ) Status on ( LS \ n )</th>
<th>Received Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP ( R )</td>
<td>TCR ( R )</td>
</tr>
<tr>
<td>none:</td>
<td>-</td>
</tr>
<tr>
<td>allowed:</td>
<td>1</td>
</tr>
<tr>
<td>restricted:</td>
<td>1</td>
</tr>
<tr>
<td>prohibited:</td>
<td>-</td>
</tr>
</tbody>
</table>

1. Change member \( z \) status for \( LS \ n \) to prohibited. Perform rerouting for member \( z \) from that route, if applicable.
2. Change member \( z \) status for \( LS \ n \) to restricted. Perform rerouting for member \( z \) from that route, if applicable.
3. Change member \( z \) status for \( LS \ n \) to allowed. Perform rerouting for member \( z \) to that route, if applicable.
4. Change member \( z \) status for \( LS \ n \) to restricted. Perform rerouting for member \( z \) to that route, if applicable.
D.5.2 Cluster Management

As discussed before, a cluster route set can only be provisioned for remote clusters. In addition, when cluster routing and management diversity is used, a member route set can be provisioned in clusters for which a cluster route set is also provisioned. This, for example, supports the concept of performing cluster routing, when an E-link set is deployed to a member of a remote cluster. This section provides detailed procedures that should be followed at the STP if a cluster route set is provisioned for the affected cluster. For cluster routing and management diversity, it also includes procedures that should be followed when an associated member route set is provisioned (see Section D.5.2.1.1).

Cluster management functionalities are divided into the following areas:

- Receipt of TFx and TCx messages
- Sending TFx and TCx messages
- Receipt of RSx and RCx messages
- Sending RSx and RCx messages.

D.5.2.1 Receipt of TFx and TCx Messages

Referring to Figure D-1, there are many situations in which STP 1 might receive either TCx messages for Cluster $R$ or TFx messages for any of its members. For example, STP A would send a TFP message to STP 1 regarding point code $x$ if links 1 and 4 failed. Or, STP C could send a TCP message to STP 1 for Cluster $R$ if it lost its normal routes for the cluster and began to route all traffic destined for Cluster $R$ via the C-link set.

Table D-2 specifies the actions the STP should take, upon receipt of TFx and TCx messages. $R$ refers to any cluster for which a cluster route set is provisioned, and $z$ refers to any member of that cluster. (For the cluster routing and management diversity [CRMD] model, $z$ refers to any member of the cluster for which a member route set is not provisioned.) All table entries that have a dash (-) are considered error conditions, so no action should be taken by the STP in those situations. The STP performs rerouting for the whole cluster to the route with the status change (i.e., for list items 1 through 4, 6, 9, 12, 13, 15, 17, 19, 21, 23 through 25), it is implied that the route to which rerouting is performed is of higher priority than or, in some cases, equal priority to the one which is currently used (controlled rerouting). If the route with the status change is of lower priority for a given destination than the one currently used, rerouting is not performed. On the other hand, for the list items 5, 7, 8, 10, 11, 14, 16, 18, 20, 22, forced rerouting is performed. In the case of
Table D-2. STP Actions Upon Receipt of TFx and TCx Messages

<table>
<thead>
<tr>
<th>Cluster R Status on LS n</th>
<th>Received Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP R</td>
<td>TCR R</td>
</tr>
<tr>
<td>prohibited:</td>
<td></td>
</tr>
<tr>
<td>x-list empty</td>
<td>-</td>
</tr>
<tr>
<td>z marked TFP on x-lista</td>
<td>-</td>
</tr>
<tr>
<td>restricted:</td>
<td></td>
</tr>
<tr>
<td>x-list empty</td>
<td>5</td>
</tr>
<tr>
<td>z marked TFR on x-listb</td>
<td>8</td>
</tr>
<tr>
<td>z marked TFP on x-list</td>
<td>11</td>
</tr>
<tr>
<td>allowed:</td>
<td></td>
</tr>
<tr>
<td>x-list empty</td>
<td>14</td>
</tr>
<tr>
<td>z marked TFR on x-list</td>
<td>18</td>
</tr>
<tr>
<td>z marked TFP on x-list</td>
<td>22</td>
</tr>
</tbody>
</table>

a. This row does not apply if a supplier does not keep prohibited x-list members for a prohibited cluster.
b. This row does not apply if a supplier does not keep restricted x-list members for a restricted cluster.

1. Change cluster R status for LS n to restricted. Perform rerouting for the whole cluster to that route.
2. Change cluster R status for LS n to allowed. Perform rerouting for the whole cluster to that route.
3. Change cluster R status for LS n to restricted. Immediately restart RSP procedures for member z. Perform rerouting for the whole cluster to that route, except for member z.
4. Change cluster R status for LS n to allowed. Immediately restart RSP procedures for member z. Perform rerouting for the whole cluster to that route, except for member z.
5. Change cluster R status for LS n to prohibited. Perform rerouting for the whole cluster from that route.
6. Change cluster R status for LS n to allowed. Perform rerouting for the whole cluster to that route.
7. Add member z to the x-list for cluster R on LS n, mark it as prohibited on LS n. Perform rerouting from that route for member z.
8. Change cluster $R$ status for LS $n$ to prohibited. Either remove member $z$ from x-list, or change its status to prohibited. Perform rerouting for the whole cluster from that route.

9. Change cluster $R$ status for LS $n$ to allowed. Immediately restart RSR procedures for member $z$. Perform rerouting to that route for all members of the cluster, except member $z$.

10. Change status of member $z$ to prohibited on the x-list. Perform rerouting from that route for member $z$.

11. Change cluster $R$ status for LS $n$ to prohibited. Either remove member $z$ from the x-list or continue to maintain its status. Perform rerouting for the whole cluster from that route, except for member $z$, which should not have any traffic on that route.

12. Change cluster $R$ status for LS $n$ to allowed. Perform rerouting to that route for all members of the cluster, except member $z$.

13. Either remove member $z$ from the x-list, or change it to restricted status. Perform rerouting for member $z$ to that route.

14. Change cluster $R$ status for LS $n$ to prohibited. Perform rerouting for the whole cluster from that route.

15. Change cluster $R$ status for LS $n$ to restricted. Perform rerouting for the whole cluster from that route.

16. Add member $z$ to the x-list for cluster $R$, mark it as prohibited for LS $n$. Perform rerouting for member $z$ from that route.

17. Add member $z$ to the x-list for cluster $R$, mark it as restricted for LS $n$. Perform rerouting for member $z$ from that route.

18. Change cluster $R$ status for LS $n$ to prohibited. Either remove member $z$ from the x-list, or mark it as prohibited. Perform rerouting for the whole cluster from that route.

19. Change cluster $R$ status for LS $n$ to restricted. Either remove member $z$ from the x-list, or continue to maintain it. Perform rerouting for the whole cluster from that route, except for member $z$.

20. Change member $z$ status to prohibited. Perform rerouting for member $z$ from that route.

21. Remove member $z$ from x-list for cluster $R$ for LS $n$. Perform rerouting for member $z$ to that route.

22. Change cluster $R$ status for LS $n$ to prohibited. Either remove member $z$ from the x-list, or continue to maintain it. Perform rerouting for the whole cluster from that route, except for member $z$, which should not have traffic on that route.

23. Change cluster $R$ status for LS $n$ to restricted. Perform rerouting for the whole cluster from that route, except for member $z$, which should not have traffic on that route.
24. Change the status of member \( z \) to restricted on x-list for cluster \( R \) for LS \( n \). Perform rerouting for member \( z \) to that route.

25. Remove member \( z \) from the x-list for cluster \( R \) for LS \( n \). Perform rerouting for member \( z \) to that route.

The above procedures that involve removing members from a cluster’s x-list upon receipt of certain TCx messages rely on the ability of the STP originating the TCx message to resend any point code exception status information (i.e., TFRs or TFPs) after it sends a new TCA or TCR. This functionality is described in Section D.5.3, *Compatibility Issues*.

### D.5.2.1.1 Additional Rules for Cluster Routing and Management Diversity

Table D-3 specifies the actions the STP should take, upon receipt of TFx and TCx messages, if a member route set is provisioned in the same cluster that a cluster route set is provisioned. Signaling point \( z \) refers to the member for which a member route set is provisioned, and \( R \) refers to the cluster to which the member belongs. All table entries that have a dash (-) are considered error conditions, so no action should be taken by the STP in those situations. For table entries indicating a route (member or cluster) status change from a more restrictive to a less restrictive status, rerouting (i.e., controlled) is performed only if the route with status change is of higher priority than or equal priority to the one which is currently used for the destination.

<table>
<thead>
<tr>
<th>Cluster ( R ) Status on LS ( n )/ Member ( z ) Status on LS ( n )</th>
<th>Received Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP ( R )</td>
<td>TCR ( R )</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>allowed /prohibited:</td>
<td>1</td>
</tr>
<tr>
<td>restricted/prohibited:</td>
<td>-</td>
</tr>
<tr>
<td>prohibited/prohibited:</td>
<td>-</td>
</tr>
<tr>
<td>allowed /restricted:</td>
<td>8</td>
</tr>
<tr>
<td>restricted/allowed:</td>
<td>8</td>
</tr>
<tr>
<td>allowed /allowed:</td>
<td>14</td>
</tr>
</tbody>
</table>

1. Change cluster \( R \) status for LS \( n \) to prohibited. Perform rerouting for every member of the cluster from that route, except for member \( z \), which should not have traffic on that route.

2. Change cluster \( R \) status for LS \( n \) to restricted. Perform rerouting for the whole cluster from that route, except for member \( z \), which should not have traffic on that route.

3. Change member \( z \) status for LS \( n \) to restricted. Perform rerouting for member \( z \) to that route.
4. Change member \( z \) status for LS \( n \) to allowed. Perform rerouting for member \( z \) to that route.

5. Change cluster \( R \) status for LS \( n \) to allowed. Perform rerouting to that route for all members of the cluster, except member \( z \), which should not have traffic on that route.

6. Change cluster \( R \) status for LS \( n \) restricted. Perform rerouting for the whole cluster to that route, except for member \( z \). Immediately restart RSP procedures for member \( z \).

7. Change cluster \( R \) status for LS \( n \) to allowed. Perform rerouting for the whole cluster to that route, except for member \( z \). Immediately restart RSP procedures for member \( z \).

8. Change cluster \( R \) status for LS \( n \) to prohibited. Change member \( z \) status for LS \( n \) to prohibited. Perform rerouting for the whole cluster (including member \( z \)) from that route.

9. Change cluster \( R \) status for LS \( n \) to prohibited. Perform rerouting for the whole cluster from that route, except for member \( z \).

10. Change member \( z \) status for LS \( n \) to prohibited. Perform rerouting for member \( z \) from that route.

11. Change member \( z \) status for LS \( n \) to allowed. Perform rerouting for member \( z \) to that route.

12. Change cluster \( R \) status for LS \( n \) to allowed. Perform rerouting for cluster \( R \) to that route. Immediately restart RSR procedures for member \( z \).

13. Change member \( z \) status for LS \( n \) to prohibited. Perform rerouting for member \( z \) from that route.

14. Change cluster \( R \) status for LS \( n \) to prohibited. Change member \( z \) status for LS \( n \) to prohibited. Perform rerouting for the whole cluster (including member \( z \)) from that route.

15. Change cluster \( R \) status for LS \( n \) to restricted. Change member \( z \) status for LS \( n \) to restricted. Perform rerouting for the whole cluster (including member \( z \)) from that route.

16. Change member \( z \) status for LS \( n \) to prohibited. Perform rerouting for member \( z \) from that route.

17. Change member \( z \) status for LS \( n \) to restricted. Perform rerouting for member \( z \) from that route.

D.5.2.2 Sending or Broadcasting TFx and TCx Messages

An STP transmits TFx and TCx messages to convey changes in the overall status of signaling points and clusters. A TFx message is transmitted to inform adjacent nodes that
a signaling point status has changed, from the perspective of the STP; a TCx message is transmitted to inform adjacent nodes that a cluster status has changed.

The following lists describe the specific conditions under which an STP should originate a TFx or TCx message:

- The STP should send a TFP message for signaling point $z$ in cluster $R$ under the following conditions:
  
  1. In response to an MSU received for $z$ when member $z$ (but NOT the entire cluster $R$) is inaccessible from the STP. In the case of cluster routing and management diversity (CRMD), this includes the situation when both member route sets and a cluster route set are provisioned in the same cluster, a member route set is not provisioned for member $z$, and another member (not member $z$) with a member route set provisioned is accessible, but the cluster route set shows that routes are unavailable for all point codes that use the cluster route set.
  
  2. When the STP begins to route (at changeover, changeback, or forced or controlled rerouting) traffic for $z$ (but NOT the entire cluster $R$) via a new adjacent STP. In this case, the TFP message is sent to the adjacent STP.
  
  3. As a broadcast to all adjacent nodes when $z$, but NOT the entire cluster $R$, becomes inaccessible from the STP, unless the option to deactivate broadcast mode is selected for the cluster of which the inaccessible destination is a member.
  
  4. Immediately after the STP transmits a TCA or TCR message for cluster $R$ to an adjacent STP, if the STP continues to route traffic for $z$ (but NOT the entire cluster $R$) via the adjacent STP, as started by the condition described in item 2. In this case, the TFP message is sent to the adjacent STP.
  
  5. Immediately after a TCA or TCR for cluster $R$ is sent to an adjacent node, if point code $z$, but NOT the entire cluster $R$, remains inaccessible from the STP, as described in item 3. In this case, the TFP message is sent to the adjacent node. Optionally, instead of sending the TFP immediately after the TCA or TCR message for cluster $R$, the STP could immediately enable response mode TFPs, after sending the TCA or TCR message. In other words, if T1.111.4/T8 is running for any point codes in the cluster when the TCA or TCR message is broadcast, it should be canceled, enabling response mode TFPs. Section D.5.3, Compatibility Issues, describes the rationale for this item.

- The STP should send a TCP message for cluster $R$ under the following conditions:
  
  1. In response to any MSU received for any member of cluster $R$ when the entire cluster is inaccessible from the STP.
  
  2. As a broadcast to all adjacent nodes when cluster $R$ becomes inaccessible from the STP, unless the option to deactivate broadcast mode is selected for the affected cluster.
3. When the STP begins to route MSUs for the entire cluster \( R \) via an adjacent STP. In this case, the TCP is sent to that adjacent STP.

- The STP should send a TFR message for point code \( z \) in remote cluster \( R \) in the following conditions:
  1. As a broadcast to all adjacent nodes, when \( z \) (but NOT the entire cluster \( R \)) becomes only accessible via alternate route(s) from the STP.
  2. Immediately after a TCA message for cluster \( R \) is sent, if point code \( z \) remains accessible only via alternate route(s) from the STP. In this case, the TFR message is sent to the adjacent node. Optionally, instead of sending the TFR immediately after the TCA message for cluster \( R \), the STP could immediately enable response mode TFRs, after sending the TCA message. In other words, if T1.111.4/T18 is running for any point codes in the cluster when the TCA message is broadcast, it should be canceled, enabling response mode TFRs. In a response mode TFR situation, a TFR is sent once per link or link set in response to the next message received on that link or link set for the destination \( z \). It should be noted that, unlike the TFP case, a TFR is sent by the response method only ONCE. Thus, if the TFR is missed, it will be lost indefinitely because it will not be resent for the second time. To provide an opportunity for such a response mode TFR message to be resent once, it is a supplier option to restart timer T1.111.4/T18, after the first response mode TFR message is sent under this situation. Section D.5.3, *Compatibility Issues*, describes the rationale for this item.

3. In the case of cluster routing and management diversity (CRMD), once per link or link set, in response to the first received message destined to member \( z \) which is only accessible via alternate route(s), if both member route sets and a cluster route set are provisioned in the same cluster, and a member route set is not provisioned for member \( z \). This case only applies when another member (not member \( z \)) with a member route set provisioned is allowed, but the cluster route set shows that only alternate routing is available for all point codes that use the cluster route set.

- The STP should send a TCR message for cluster \( R \) when cluster \( R \) becomes accessible only via alternate route(s) from the STP. In this case, the TCR should be broadcast to all adjacent nodes. Any running T1.111.4/T8 timers for any cluster members shall be canceled at this time, so that the response mode TFP procedures are active, immediately after broadcasting the TCR message.

- The STP should send a TFA message for point code \( z \) in cluster \( R \) under the following conditions:
  1. When the STP stops routing (at changeback or controlled rerouting) traffic for member \( z \) of cluster \( R \) via an adjacent STP. In this situation, the TFA message should be sent to the adjacent STP.
  2. As a broadcast to all adjacent nodes when \( z \) first becomes accessible via normal route(s) from the STP unless there is a change in the cluster’s status. When cluster
routing and management diversity is used, a broadcast is performed when a member provisioned with a member route set becomes accessible via normal route(s), unless the change in the member’s status also caused a change in the cluster’s status. This case does not apply if the option to deactivate broadcast mode is selected for the cluster of which the destination \( z \) is a member.

- The STP should send a TCA message for cluster \( R \) under the following conditions:
  1. When the STP stops routing traffic for the entire cluster \( R \) via an adjacent STP. In this situation, the TCA message is sent to the adjacent STP.
  2. As a broadcast to all adjacent nodes, when cluster \( R \) becomes accessible via normal route(s) from the STP, unless the option to deactivate broadcast mode is selected for the affected cluster. Any running T1.111.4/T8 and T1.111.4/T18 timers for any cluster members shall be canceled at this time, so that the response mode TFP and TFR procedures are active, immediately after the broadcast of the TCA message.

\[ D.5.2.2.1 \quad \text{Sending TFP/TCP Messages Upon Receipt of an Undeliverable Message} \]

Table D-4 summarizes whether the STP should send a TFP or TCP message upon receipt of an undeliverable message. The word none is used to indicate that either a member route set is not provisioned for the member for which the arrived message is destined to or no cluster route set is provisioned for the cluster to which the member belongs. The dash (-) in one table entry indicates that the member’s status is not used in determining which type of route management message should be sent as a response because the cluster’s status is inaccessible.

\[ \text{Table D-4. STP Messages Upon Receipt of Undeliverable Message} \]

<table>
<thead>
<tr>
<th>Cluster Status</th>
<th>Member Status</th>
<th>Message Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>none</td>
<td>TFP (1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP (2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP (3)</td>
</tr>
<tr>
<td>none</td>
<td>inaccessible</td>
<td>TFP (4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP (5)</td>
</tr>
<tr>
<td>inaccessible</td>
<td></td>
<td>TFP (6)</td>
</tr>
<tr>
<td>accessible</td>
<td>none</td>
<td>TFP (5)</td>
</tr>
<tr>
<td></td>
<td>inaccessible</td>
<td>TFP (6)</td>
</tr>
</tbody>
</table>

1. Another member of cluster exists, and the supplier option of sending TCP is not implemented when all members of cluster are inaccessible.
2. No members of cluster exist. (As a non-preferred option, TFP message may be sent instead.)

3. A supplier option. Other members of cluster exist and are all inaccessible.

4. A supplier option. No cluster member is inaccessible.

5. The member is marked prohibited on the x-lists corresponding to available or restricted cluster routes.

6. The member is marked prohibited over all routes in the member route set.

D.5.2.3 Sending Signaling-Route-Set-Test Messages

An STP begins sending signaling-route-set-test messages in response to received TCx (i.e., TCP or TCR) or TFx (i.e., TFR or TFP) messages. RSx (i.e., RSR or RSP) or RCx (i.e., RCR or RCP) message should only be sent in response to received TFx or TCx messages if the TFx or TCx message concerns a route in the route set that the STP uses for routing traffic to the affected point code or cluster. They should be sent to the originator of the TFx or TCx messages.

The conditions under which an STP should send RSx or RCx messages, and under which it should stop sending the RSx and RCx messages follow.

1. An STP should send an RCP message for cluster \( R \), in response to a TCP message received for the cluster from an adjacent STP. The STP should continue sending the RCP messages, every T1.111.4/T10 seconds, until the STP receives either a TCA or TCR message for cluster \( R \) from the adjacent STP.

2. An STP should send an RCR message for cluster \( R \) in response to a TCR message received for the cluster from an adjacent STP. The STP should continue sending the RCR messages, every T1.111.4/T10 seconds, until it receives a TCP or TCA message for cluster \( R \) from the adjacent STP.

3. An STP should send an RSP message for member \( z \) of cluster \( R \) when the status of the cluster is allowed or restricted on a given cluster route (according to the cluster route set), and a TFP message for \( z \) is received concerning that route. In addition, an RSP message should be sent when a TCA or TCR message is received about cluster \( R \), and the status of member \( z \) remains prohibited on the route (for example, an RSP message will be sent when the cluster was previously marked prohibited or restricted on a given cluster route and member \( z \) was marked prohibited on the x-list corresponding to that cluster route, or in the case of cluster routing and management diversity, when a member route set is provisioned for member \( z \) and the member is marked prohibited on the associated member route). The STP should continue sending the RSP messages, every T1.111.4/T10 seconds, until it receives one of the following messages from the originator of the original TFP message:
• A TCP message for cluster $R$
• A TFA or TFR message for $z$.

4. An STP should send an RSR message for member $z$ of cluster $R$ when the status of the cluster $R$ is allowed on a given route (according to the cluster route set), and a TFR message for $z$ is received concerning that route. In addition, an RSR message shall be sent when a TCA message is received about cluster $R$, and the status of the member remains restricted (for example, an RSR message will be sent when the cluster was previously marked restricted on a given cluster route and member $z$ was marked restricted on the x-list corresponding to that cluster route, or in the case of cluster routing and management diversity, when a member route set is provisioned for member $z$ and the member is marked restricted on the associated member route). The STP should continue sending the RSR messages, every T1.111.4/T10 seconds, until it receives one of the following messages from the originator of the original TFR message.

• A TFA or TFP message for $z$
• A TCR or TCP message for cluster $R$.

Table D-5 summarizes the criteria to send a particular test message. In the case of cluster routing and management (CRM), the status of the cluster route and a member $z$ on the cluster route determine which test message(s) should be sent. In the case of cluster routing and management diversity (CRMD), if the member $z$ has an associated member route, then the test message sent is determined based on the status of the cluster route and the associated member route. The word _none_ is used to indicate that information corresponding to a destination does not exist. Specifically, for the cluster, _none_ indicates that the STP has no cluster route set provisioned for the cluster of which $z$ is member. This is the case when the STP does full point code routing to every member of the cluster. When _none_ is used to indicate the status of $z$, it means that no entry exists for $z$ on the x-list associated with the cluster and the route, and, in the case of cluster routing and management diversity, _none_ is also used to mean that a member route set is not provisioned for $z$.

<table>
<thead>
<tr>
<th>Cluster Status on Ls $n$</th>
<th>Status of Member $z$ on Ls $n$</th>
<th>Test Message Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>none</td>
<td>allowed</td>
<td>none</td>
</tr>
<tr>
<td>none</td>
<td>restricted</td>
<td>RSR</td>
</tr>
<tr>
<td>none</td>
<td>prohibited</td>
<td>RSP</td>
</tr>
<tr>
<td>allowed</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>allowed</td>
<td>allowed</td>
<td>none</td>
</tr>
<tr>
<td>allowed</td>
<td>restricted</td>
<td>RSR</td>
</tr>
</tbody>
</table>
D.5.2.4 Receiving Route Set Test Messages

An STP sends a TEn or TCn message, in response to received RSx and RCx messages, when the status of the signaling point or cluster on the affected route is different from the status indicated in the RSx or RCx message. Note that when a member has an exception to the cluster status, that member may either be on the cluster’s x-list(s), or, in the case of cluster routing and management diversity (CRMD), a member route set may be provisioned for that member, indicating that the member has a different status on the associated member route than the status indicated in the cluster route set for the cluster.

Table D-6 summarizes the actions that the STP should take upon receipt of RSx and RCx messages. All table entries that have a dash (-) indicate that no action should be taken, because the destination status matches that in the received RSx or RCx message. Note that the table below does not apply if a preventive TFP/TCP message about an affected destination is sent to an adjacent STP, and an RSP/RCP message is received about that affected destination from that adjacent STP.

### Table D-6. STP Actions Upon Receipt of Test Messages

<table>
<thead>
<tr>
<th>Cluster Status on Ls n</th>
<th>Status of Member z on Ls n</th>
<th>Test Message Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>allowed</td>
<td>prohibited</td>
<td>RSP</td>
</tr>
<tr>
<td>restricted</td>
<td>none</td>
<td>RCR</td>
</tr>
<tr>
<td>restricted</td>
<td>restricted</td>
<td>RCR</td>
</tr>
<tr>
<td>restricted</td>
<td>prohibited</td>
<td>RCR and RSP</td>
</tr>
<tr>
<td>prohibited</td>
<td>none</td>
<td>RCP</td>
</tr>
<tr>
<td>prohibited</td>
<td>prohibited</td>
<td>RCP</td>
</tr>
</tbody>
</table>

D-23
The numbers below correspond to those in the above table. All messages are sent to the originator of the RSx or RCx message.

1. Send a TCP message for cluster \( R \).
2. Send a TFP message for member \( z \).
3. Send a TCR message for cluster \( R \).
4. Send a TFR message for member \( z \).
5. Send a TCR message for cluster \( R \), followed by a TFP message for member \( z \).
6. Send a TCA message for cluster \( R \).
7. Send a TFA message for member \( z \).
8. Send a TCA message for cluster \( R \), followed by a TFR message for member \( z \).
9. Send a TCA message for cluster \( R \), followed by a TFP message for member \( z \).

**D.5.3 Compatibility Issues**

Since not all nodes will be performing cluster routing for the same clusters, there may be times when mismatches may occur. It is an objective to minimize any problems that could result due to these mismatches, in order to ensure that network integrity is maintained.

Consider the possibility, in Figure D-2, that the RSTP mated pair is provisioned with only member route sets for every member of Cluster L. Assume that the LSTP 1 mated pair is only provisioned with a cluster route set for Cluster L. There are times when LSTP 1 or its mate may transmit TCx messages to the RSTP pair. First, assume that some individual members of Cluster L go down, so LSTP 2 and its mate will convey this information to LSTP 1 via TFP messages. Upon receiving those TFP messages, LSTP 1 will place the members on the x-list for Cluster L. Second, assume all normal and alternate routes from LSTP 1 to Cluster L go down, so LSTP 1 will send a TCP message to the RSTP pair for Cluster L. In the meantime, LSTP 1 continues to maintain the signaling route status for Cluster L over all routes, even though the local link sets corresponding to the routes are

---

<table>
<thead>
<tr>
<th>Cluster ( R ) Status on ( L ) ( n )</th>
<th>Received Message</th>
<th>RCP ( R )</th>
<th>RCR ( R )</th>
<th>RSP ( z )</th>
<th>RSR ( z )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( z ) restricted</td>
<td>8</td>
<td>8</td>
<td>4</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>( z ) prohibited</td>
<td>9</td>
<td>9</td>
<td>-</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>-</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

* When the overall routing status is more restrictive than the cluster status.
unavailable. Now, since the RSTP pair maintains route status information for every
member of Cluster L, upon receiving the TCP message, they will mark every member of
Cluster L for which there is a member route set provisioned as prohibited on the route.

Third, assume that the normal routes to Cluster L are then restored, so LSTP 1 will send a
TCA to the RSTP pair for Cluster L. The RSTP pair will then mark every member of
Cluster L as allowed on the route, even though some individual members of Cluster L may
be prohibited. To deal with that undesirable situation, LSTP 1, after sending the TCA to the
RSTP pair, should be able to inform adjacent nodes of the restricted and prohibited status
of members of cluster L. This may be done in one of two ways. TFP and TFR messages
may be sent on each link over which a corresponding TCA message is sent, immediately
after the TCA message; or, LSTP 1 may send response mode TFP and TFR messages after
sending the TCA message on each link, so that any subsequent traffic destined toward a
restricted or prohibited destination is immediately responded to with a TFR or TFP
message. In this case, LSTP 1, after sending the TCA message, must cancel any running
T1.111.4/T8 timer for the prohibited members of cluster L and T1.111.4/T18 timer for the
restricted members to ensure that response mode TFP and TFR messages will be sent
immediately after the TCA message. As a supplier option, it may also be desirable to restart
timer T1.111.4/T18, after the first TFR message is sent in the response mode, to provide an
opportunity for the TFR message to be resent once, if the first TFR message is lost or not
acted upon. Similarly, after LSTP 1 transmits a TCR message to the RSTP pair for Cluster
L, it should be able to inform adjacent nodes of the prohibited status of members of cluster
L. Again, this may be done in one of two ways. TFP messages may be sent over each link
over which a corresponding TCR message is sent, immediately after the TCR message; or,
LSTP 1 may send response mode TFP messages after sending the TCR message on each
link, so that any subsequent traffic destined toward a prohibited destination is immediately
responded to with a TFP message. In this case, LSTP 1, after sending the TCR message,
must cancel any running T1.111.4/T8 timer for the prohibited members of cluster L to
ensure that response mode TFP messages will be sent immediately after the TCR message.

These mechanisms will provide the RSTP pair with a way to determine the correct routing
status of all members of Cluster L.

In the above scenario, it is only possible for LSTP 1 to send the TFP messages after the
TCA message, if LSTP 1 maintains route status information while the links corresponding
to a route remain unavailable. This capability is possible because of the requirement that
signaling route management messages be sent over any available or restricted route to a
destination, permitting a node to maintain route status information for unavailable routes,
if the destination is accessible via other routes. If, however, the destination is inaccessible,
i.e., all the routes to the destination are unavailable, then the MTP restart procedures are
started when a route to the destination first becomes accessible. Those procedures allow the
STP to update its routing tables (including x-lists), so after they are run, the STP is once
again able to broadcast exceptions to cluster route status.
D.5.4 Interaction with SS7 Congestion Control

The Bellcore specification of SS7 provides procedures for congestion control in the SS7 network. Signaling route set congestion procedures are initiated in response to the following events:

- Indication of local signaling link transmit congestion
- Receipt of a Transfer-Controlled (TFC) message
- Receipt of a signaling-route-set-congestion-test message.

D.5.4.1 Local Link Congestion

Local link congestion is a Level 2 function; it has no interaction with cluster management.

D.5.4.2 Transfer-Controlled (TFC) Messages

A TFC message is sent by an STP in response to a received MSU when the priority of the concerned message is less than the current congestion status of the signaling link selected to transmit the MSU. The TFC sent to the originating node should indicate as the affected point code the DPC of the message that triggered the TFC.

D.5.4.3 Signaling-Route-Set-Congestion-Test Procedures

Signaling-route-set-congestion-test procedures are initiated in response to receipt of a TFC message. When a TFC message arrives at the SP indicated in the OPC field of the TFC message, T1.111.4/T15 timer is started at the SP. Upon expiration of the timer, the SP sends a RCT message destined to the affected destination (i.e., the congested destination indicated in the TFC message) periodically, with an interval of T1.111.4/T16, until the congestion status of the affected destination abates. The RCT message to the affected destination is sent on a route set basis, not on an individual route basis. In the case of SCCP routing involving global title translation, the STP performing the last global title translation on a query becomes the originator of the query (i.e., the OPC field of the query contains the STP’s point code.) and if the query then encounters congestion on its way to the final destination, the originating STP receives a TFC message. This STP then must be able to send a RCT message to check the congestion status level of the route set corresponding to the final destination, even though, at the MTP level, the STP may not maintain individual routing statuses for each point code in remote clusters to which it can translate global title query messages. Thus, the STP must have full point code information in its global title translation tables (to correctly assign DPCs to outbound query messages), but does not necessarily have to maintain routing statuses for every one of these point codes. Therefore,
full point code information could be provisioned with a cluster route set for point codes to which it translates global title messages.

The STP must be able to accomplish the following actions upon receiving the TFC, even if a member route set is not provisioned for the affected point code:

- Mark the route set to that destination as congested with the congestion level that is indicated in the received TFC message.
- Send an RCT every T1.111.4/T16 seconds and decrement the congestion level associated with the destination if no TFC is received in reply. If a TFC is received, restart T1.111.4/T15.
- Stop originating global title queries or subsystem management messages to the affected destination with priorities less than the current congestion level associated with that destination. This could be accomplished either by having the MTP inform the SCCP of the congestion level so that SCCP takes action, or by having the MTP discard messages without informing the SCCP.

D.5.5 Interaction with MTP Restart

The cluster management procedures described in Section D.5.2 should appropriately interact with MTP restart procedures described in T1.111.4. In addition to exchanges of TFP and TFR messages between the restarting node and the adjacent node, TCP and TCR messages should be accounted for during the restarting process, when appropriate. The status of routes at the restarting STP should be appropriately recorded based on TCx messages received. Received TFP and TFR messages both should be used to add point codes to the x-lists and broadcasted to adjacent nodes prior to resuming normal operation. In the above descriptions, it is assumed that the restart procedures are initiated when a node is isolated from the far end and the contents of the x-lists are cleared before the initiation of the restart process.

D.5.6 Interaction With the SCCP Layer

The SCCP management functions provide the procedures necessary to maintain network performance by rerouting traffic in the event of failures in the network.

SCCP management consists of point code management and subsystem management. Each of these is discussed below.
D.5.6.1 Point Code Status Management

Point code status management allows routing and translation tables to be updated in response to failures, recoveries, or congestion of nodes in the network.

- An MTP-PAUSE indication should be sent to SCCP management under the following circumstances:
  - When a cluster becomes inaccessible, the primitive is sent for the cluster as a whole. SCCP management should mark its tables so that every member of the concerned cluster is treated as inaccessible. SCCP management must maintain full point code status tables.
  - When individual members of cluster R become inaccessible, an MTP-PAUSE is sent for each individual point code.

When SCCP management receives either of these indications, it should take the actions specified in Section 5.2.2 of T1.112.4 in GR-246-CORE.

- An MTP-RESUME indication should be sent to SCCP management under the following circumstances:
  - If a member of a cluster was previously inaccessible, the primitive should be sent when it becomes accessible.
  - When the entire cluster becomes accessible, the primitive should be sent for the cluster as a whole. SCCP management should mark each point code in the cluster as accessible.

When SCCP management receives either of these indications, it should take the actions specified in T1.112.4, Section 5.2.3.

D.5.6.2 Subsystem Status Management

There is no interaction between cluster management and SCCP subsystem management. MTP network management is not concerned with the statuses of individual subsystems at nodes. Therefore, this information is not contained in either the cluster statuses or x-lists, so there is no communication required to the subsystem management.
Figure D-1. Model Network Configuration
Figure D-2. Three-Level Architecture Model
Appendix E: STP Requirements for SCCP ISNI

Appendix E describes Bellcore’s view of the SCCP Intermediate Signaling Network Identification (ISNI) capability.

E.1 Introduction

The SCCP ISNI capability allows an application process in the originating network to specify intermediate signaling network(s) for non-circuit associated signaling messages and to notify an application process in the terminating network about such intermediate signaling network(s). The SCCP ISNI capability may be invoked by a variety of services.

As an example of non-circuit related messages supporting the operation of a feature, suppose an end user activates a CLASS feature, such as Automatic Recall. The originating central office first determines whether the called party’s line is busy or idle by sending a non-circuit related message over the CCS network to the terminating central office. If the response message indicates that the called party’s line is idle, the call is completed. If the response message indicates that the called party’s line is busy, the originating or terminating central office monitors the called party’s line by exchanging additional messages.

Development of the SCCP ISNI capability began to satisfy the need for the network capability of specifying interconnecting CCS network (ICNs) to carry the non-circuit related query and response messages in addition to the ability of notifying the responding network of the sequence of one or more ICNs traversed by an initial query. The SCCP ISNI capability defines a parameter in the SCCP portion of the message, called the SCCP ISNI parameter, to accomplish these tasks.

The organization of this appendix begins with definitions in Section E.2. Section E.3 describes the format and coding of the SCCP ISNI parameter. Section E.4 explains the notation used in Sections E.5 and E.6. Section E.5 describes the procedures for routing messages with the SCCP ISNI parameter, including the procedures for routing service messages. Examples of the formatting and coding of the Type 1 SCCP ISNI parameter are included in Section E.6. The operations requirements for SCCP ISNI in Section E.7 include provisioning and administration capabilities.

E.2 Definition of Terms

The following terms are used throughout Appendix E:

- Originating Network—The network that generates the non-circuit related message that requires the use of the SCCP ISNI capability.
• Terminating Network—The network that receives the non-circuit related message that requires the use of the SCCP ISNI capability.

• Interconnecting CCS Network (ICN)—A CCS network, other than the originating and terminating networks, that may carry the non-circuit related message.

• Constrained ISNI Routing—If a feature requests that the message’s route be constrained to the sequence of ICN(s) in the SCCP ISNI parameter, the message must follow the specified route or the message will fail.

• Suggested ISNI Routing—Suggested ISNI Routing, still under study, would allow a network to use the routing information in the SCCP ISNI parameter as a recommendation for the next network. The message is not required to follow the specified path. As such, no requirements for this type of routing are provided here.

• Neither Constrained Nor Suggested ISNI Routing—If an STP receives a message sent with Neither Constrained Nor Suggested ISNI Routing, the SCCP ISNI parameter does not indicate any routing instructions. The STP will perform a global title translation (GTT) on the SCCP Called Party Address, as GR-246-CORE defines, to forward the message towards the terminating Signaling End Point (SEP).

• ISNI Identification—If the feature requests that each network that the message traverses performs identification, then each network records its identifier in the SCCP ISNI parameter (if not already present). Thus, the information delivered to the terminating SEP is the documentation of the actual sequence of networks.

• Carrier Identification Code (CIC)—The interexchange carrier is identified by its CIC. The CIC is assigned to a carrier by the North American Numbering Plan. The CIC is a number from 0 to 999, and may be extended to 9999 in the future. See GR-690-CORE, Exchange Access Interconnection, for more information.

### E.3 Format and Coding of the SCCP ISNI Parameter

**RE-1 [479]** The SCCP ISNI parameter shall be formatted and coded as shown in Table E-1.
Table E-1. SCCP Intermediate Signaling Network Identification Parameter

<table>
<thead>
<tr>
<th></th>
<th>h</th>
<th>g</th>
<th>f</th>
<th>e</th>
<th>d</th>
<th>c</th>
<th>b</th>
<th>a</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SCCP ISNI Parameter</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Parameter Length</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>Counter</td>
<td>Type of Parameter</td>
<td>Res.</td>
<td>Type of Routing</td>
<td>MI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Network Specific</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Network Identifier 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Network Identifier 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Network Identifier K</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A. SCCP ISNI Parameter—This field indicates that the SCCP optional parameter to follow is the SCCP ISNI parameter. The parameter identifier for the SCCP ISNI parameter is “1111 1010.”

B. Parameter Length—The length of the SCCP ISNI parameter in this message is variable and will depend on the SCCP ISNI parameter type and the number of network identifiers in the parameter.

C. Routing Control Indicator—This field indicates the type of routing control requested for the message. The fields in the Routing Control Indicator are:
• Counter—The Counter provides an imaginary “pointer” which is used to locate routing and identification information. The Counter identifies the number of network identifiers contained in the Network Identifier Field as identification information. Any network identifiers after the identification information provide routing information. Thus, if the value of the Counter is three, then the first three network identifiers provide identification information, and any additional network identifiers provide additional routing information. The Counter has a maximum value of seven. See Section E.4 for an example of how the Counter is used as a pointer.

• Type of SCCP ISNI Parameter—Two types of SCCP ISNI parameters have been defined. The ‘Type 0’ SCCP ISNI parameter does not include the Routing Control Extension Octet, and the ‘Type 1’ SCCP ISNI parameter does.

• Reserved—This field is reserved for extension to the Type of ISNI Routing field.

• Type of ISNI Routing—This field indicates the type of ISNI routing requested by the feature in the originating network.

    Type of ISNI Routing  00  Neither Constrained Nor Suggested ISNI Routing
    01  Constrained ISNI Routing
    10  Reserved for Suggested ISNI Routing
    11  Reserved

• Mark for Identification (MI)—This field indicates whether or not the feature in the originating network requests the networks to identify themselves in the message.

    MI  0  Do Not Identify Networks
        1  Identify Networks

D. Routing Control Extension—If the parameter included in the message is a Type 0 SCCP ISNI parameter, the Routing Control Extension octet is not included in the parameter. If the parameter included in the message is a Type 1 SCCP ISNI parameter, this octet is included in the parameter. Only one field has been defined in the Routing Control Extension as the Network Specific Indicator. The remainder of the octet is spare.

• Network Specific—This field identifies the coding format used for the information in the Network Identifier field. The CIC is a binary coded decimal representation of the three or four digit number that identifies the ICN. The Null ICN Identity is coded as two octets of zeros that serve as a placeholder for the true ICN identity.
A network identifier encoded in SS7 format is a combination of “network codes” plus “cluster codes” as T1.111.4 of GR-246-CORE defines. Tables E-2 and E-3 in Section E.6 show examples of the coding of the Type 1 SCCP ISNI parameter with the CIC and the Null ICN Identity in the Network Identifier Field.

E. Network Identifiers—The information in the Network Identifier fields specifies the routing and identification information. If the parameter included in the message is a Type 0 SCCP ISNI parameter, the information is encoded in SS7 format. If the parameter is a Type 1 SCCP ISNI parameter, the Network Specific Indicator identifies the coding format of the information. The SCCP ISNI parameter can hold up to seven network identifiers.

If a network is large and the identifier is encoded in SS7 format, the “cluster code” may be coded all 0s (i.e., “00000000”) or may be coded with the non-zero cluster code of a particular node within the large network. It should be noted that a Bcc STP will use both its network code and non-zero cluster code when performing SCCP ISNI identification. If a network is small, the identifier will consist of both the “network code” and “cluster code” that uniquely identify the small network.

E.4 Notation

For these procedures, the Counter in the Routing Control Indicator octet shall be used to identify specific octets of information in the Network Identifier field.

The Counter value shall be designated by the letter “P.” In addition, the following notation is used:

- The notation “2 + 2P” indicates the number of the octet following the Parameter Length octet.
- Octet numbers in curly brackets, {}, refer to the octet with the Type 0 SCCP ISNI parameter.¹
- Octet numbers in square brackets, [], refer to the octet with the Type 1 SCCP ISNI parameter.

1. Recall that the Type 0 SCCP ISNI parameter does not contain the Routing Control Extension octet, and the Type 1 SCCP ISNI parameter does.
• If the octet numbers do not appear in any brackets, the number applies to both the Type 0 and the Type 1 parameters.

Thus, if the value of the Counter is 1 (i.e., P=1), then \{2+2P\} indicates the fourth octet after the Parameter Length octet in the Type 0 parameter, which is the “network code” of the second network identifier (in SS7 format) in the Network Identifier Field. Recall that the first network identifier, in the second and third octets of the parameter, provides identification information. The network identifier in the fourth and fifth octets is the first identifier in the routing information (there may be additional identifiers in the routing information).

E.5 SCCP ISNI Message Routing Procedures

The SCCP ISNI Message Routing Procedures specify the overall actions of the STP when the STP receives a message that includes the SCCP ISNI parameter. The procedures begin by translating any ICN information in the SCCP ISNI parameter to SS7 format in the SCCP ISNI Network Specific Procedures in Section E.5.1. The STP then performs the SCCP ISNI Constrained Routing and Identification Procedures, in Sections E.5.2 and E.5.3, as required. If the STP receives an XUDTS message with the SCCP ISNI parameter, the STP performs the SCCP ISNI Error Message Routing Procedures in Section E.5.4.2.

If the STP receives an XUDT message with a Type 1 SCCP ISNI parameter, and the Network Specific indicator is not set to “00,” then the network identifier(s) in the SCCP ISNI parameter is not in SS7 format. The STP shall perform the following procedures:

RE-2 [480] To determine a network identifier(s) in SS7 format, the STP shall perform the SCCP ISNI Network Specific Procedures in Section E.5.1.

RE-3 [481] Upon completion of the SCCP ISNI Network Specific Procedures, the STP shall perform the following procedures:

… A. If the Type of ISNI Routing indicator is set to Suggested ISNI Routing or Reserved, the message shall fail due to an invalid SCCP ISNI routing request. The STP shall perform the SCCP ISNI Error Message Procedures as described in Section E.5.4.

… B. If the Type of ISNI Routing indicator is set to Constrained ISNI Routing² or Neither Constrained Nor Suggested ISNI Routing, the STP shall perform the following procedures:

² The SCCP ISNI Constrained Routing Procedures will be performed as part of the Network Specific Procedures, if necessary.
• If the Mark for Identification indicator is set to “Identify Networks,” the STP shall perform the SCCP ISNI Identification Procedures in Section E.5.3.

• If the Mark for Identification indicator is set to “Do Not Identify Networks,” the STP has completed the ISNI Message Routing Procedures.

RE-4 [482] If the STP receives an XUDT message with a Type 0 SCCP ISNI Parameter, or a Type 1 SCCP ISNI Parameter with the Network Specific indicator set to “00,” the information in the Network Identifier field is in SS7 format. The STP shall perform the following procedures:

1. If the Type of ISNI Routing indicator is set to Constrained ISNI Routing, the STP shall complete the SCCP ISNI Constrained Routing Procedures in Section E.5.2.

2. If the Type of ISNI Routing indicator is set to Suggested ISNI Routing or Reserved, the message shall fail due to an invalid SCCP ISNI routing request. The STP shall perform the SCCP ISNI Error Message Procedures as described in Section E.5.4.

3. If the Type of ISNI Routing indicator is set to Neither Constrained Nor Suggested ISNI Routing, the STP shall perform the following procedures:

   • If the Mark for Identification indicator is set to “Identify Networks,” the STP shall perform the SCCP ISNI Identification Procedures in Section E.5.3.

   • If the Mark for Identification indicator is set to “Do Not Identify Networks,” the STP has completed the ISNI Message Routing Procedures.

RE-5 [483] If the STP has not determined a DPC as a result of the ISNI Message Routing Procedures, the STP shall perform a GTT on the SCCP Called Party Address as T1.112.4 of GR-246-CORE defines, to determine a DPC, and perform the following procedures:

1. If the STP cannot perform a GTT on the SCCP Called Party Address to determine a DPC, the message shall fail due to a GTT-specific cause (see Section 3.12 of T1.112.3 for a complete list of return causes). The STP shall perform the SCCP ISNI Error Message Procedures in Section E.5.4.

3. The DPC may be a point code of an individual STP or the capability code of an STP pair as described in Section 4.2.2.1.1.
2. If GTT on the SCCP Called Party Address results in a PC and SSN within the STP’s network, the STP shall verify the ability of the PC and SSN to properly process an XUDT message containing an SCCP ISNI parameter through the use of the “SCCP Application Entity,” defined in Section 5.2.3.3 and in Appendix J, Section J.2. An attribute of this entity shall identify a PC and SSN’s ability to process an XUDT message containing an SCCP ISNI parameter.

3. If the STP determines that the PC and SSN cannot properly process the message, the message shall fail due to “unauthorized message.” The STP shall perform the SCCP ISNI Error Message Procedures in Section E.5.4.

RE-6 [484] If the STP receives an XUDTS message with the SCCP ISNI parameter, the STP shall perform the SCCP ISNI Error Message Routing Procedures in Section E.5.4.2.

Figure E-1 shows the SCCP ISNI Message Routing Procedures.
Figure E-1. SCCP ISNI Message Routing Procedures
E.5.1 SCCP ISNI Network Specific Procedures

When the STP receives an XUDT message with the SCCP ISNI Parameter, the ICN information in the SCCP ISNI parameter may not be in SS7 format. Depending on the Network Specific indicator, the ICN information could also be in CIC format or the Null ICN Identity. Before the message can leave the originating network, the ICN information must be translated to SS7 format. The SCCP ISNI Network Specific Procedures translate the ICN information to SS7 format so that the STP can complete the SCCP ISNI routing and identification procedures.

RE-7 If the SCCP ISNI parameter is a Type 1 SCCP ISNI parameter and the Network Specific indicator in the Routing Control Extension octet is not set to “00,” then the information in the Network Identifier Field is not in SS7 format. The STP shall perform the SCCP ISNI Network Specific Procedures as follows:

1. If the Network Specific indicator in the Routing Control Extension octet is set to “01,” the information in the Network Identifier Field is in CIC format. The STP shall translate the ICN information to SS7 format by performing the following procedures:

   A. The STP shall map the ICN information, in CIC format, to network identifier(s) in SS7 format.

   B. If the ICN information, in CIC format, does not map to network identifier(s) in SS7 format, the message shall fail due to “invalid SCCP ISNI routing request.”

   The STP shall perform the SCCP ISNI Error Message Procedures as defined in Section E.5.4.

   C. The STP shall replace the ICN information in CIC format with the ICN information in SS7 format in the Network Identifier Field of the SCCP ISNI Parameter.

   D. The STP shall set the Network Specific indicator to “00” to indicate that the ICN information is in SS7 format.

   E. If the Type of ISNI Routing indicator is set to Constrained ISNI Routing, the STP shall complete the SCCP ISNI Constrained Routing Procedures in Section E.5.2.

   F. If the Type of ISNI Routing indicator is not set to Constrained ISNI Routing, the STP has completed the SCCP ISNI Network

---

4. Recall from the format and coding of the SCCP ISNI parameter, Section E.3, that a large network is identified by the first octet (i.e., Network Id) only. The second octet (i.e., Cluster Id) can be coded all zeros (i.e., “00000000”) or may be coded with a non-zero code.
Specific Procedures and shall complete the remaining SCCP ISNI Message Routing Procedures in Section E.5.

2. If the Network Specific indicator in the Routing Control Extension octet is set to “10,” the information in the Network Identifier Field is the Null ICN Identity. Since the Null ICN Identity is two octets of zeros and does not identify a network, the STP shall determine an ICN identity by performing the following procedures:

A. If the information in the Network Identifier Field is not two octets of zeros, the Null ICN Identity is not contained in the SCCP ISNI parameter as indicated by the Network Specific indicator. The message shall fail due to an “invalid ISNI routing request.”

The STP shall perform the SCCP ISNI Error Message Procedures as defined in Section E.5.4.

B. The STP shall perform a GTT on the SCCP Called Party Address as defined in T.1.112.4 of GR-246-CORE.

If the STP can not perform a GTT, the message shall fail due to a GTT-specific cause. The STP shall perform the SCCP ISNI Error Message Procedures in Section E.5.4.

C. The STP shall extract the ICN identifier from the DPC resulting from the GTT. The ICN identifier, in SS7 format, is the first two octets of the DPC.

D. The STP shall replace the Null ICN Identity, in the Network Identifier Field, with the ICN identifier extracted from the DPC.

E. The STP shall set the Network Specific indicator to “00” to indicate that the ICN information is in SS7 format.

F. The STP has completed the SCCP ISNI Network Specific Procedures and shall complete the remaining SCCP ISNI Message Routing Procedures in Section E.5.

3. If the Network Specific indicator in the Routing Control Extension octet is set to “11,” the format of the information in the Network Identifier Field is unknown. The message shall fail due to an “invalid SCCP ISNI routing request.” The STP shall perform the SCCP ISNI Error Message Procedures in Section E.5.4.

Figure E-2 shows the SCCP ISNI Network Specific Procedures.
SCCP ISNI Network Specific Procedures

Is the Network Specific Indicator set to "01"?

Y

Map the identifier in CIC format to SS7 format

N

Is the Network Specific Indicator set to "10"?

Y

Replace the identifier in CIC format with the identifier in SS7 format in the SCCP ISNI Parameter. Reset the Network Specific Indicator to "00".

N

Perform SCCP GTT Procedures

error

Extract identifier from DPC. Replace "Null" ICN Identity with the identifier extracted from the DPC in the SCCP ISNI Parameter. Reset the Network Specific Indicator to "00."

Perform SCCP ISNI Constrained Routing Procedures

Is the Type of ISNI Routing set to Constrained ISNI Routing?

Y

SCCP ISNI Network Specific Procedures complete

N

Is the Type of ISNI Routing set to Constrained ISNI Routing?
E.5.2 SCCP ISNI Constrained Routing Procedures

If a message’s route is constrained to the sequence of network(s) in the SCCP ISNI parameter, the message must follow the specified route or the message will fail. With the help of the Counter, the STP will locate the first network identifier in the routing information, if routing information is available. If the first network identifier in the routing information identifies the STP’s network, the STP moves the identifier from routing information to the identification information by incrementing the Counter. Note that if the STP’s network identifier is listed in the routing information twice, the message will fail due to redundant routing information.

After the STP moves its network identifier to the identification information, additional routing information may or may not be available in the parameter. If additional routing information is available, the STP determines a DPC based on the first network identifier in the routing information. If additional routing information is not available, the STP will perform a GTT on the SCCP Called Party Address.

Recall that P is the value of the Counter for these procedures.

RE-8 [486] If the Type of ISNI Routing indicator is set to Constrained ISNI Routing, and the length of the SCCP ISNI parameter is not greater than 2 + 2P, then routing information is not present in the SCCP ISNI parameter. The STP shall perform the following procedures:

… 1. If the Mark for Identification indicator is set to “Identify Networks,” the STP shall perform the SCCP ISNI Identification Procedures in Section E.5.3.

… 2. If the Mark for Identification indicator is set to “Do Not Identify Networks,” the STP has completed the SCCP ISNI Message Routing Procedures.

… 3. To determine a DPC, the STP shall perform a GTT on the SCCP Called Party Address as T1.112.4 of GR-246-CORE describes.

…  • If the STP can not perform a GTT, the message shall fail due to a GTT-specific cause. The STP shall perform the SCCP ISNI Error Message Procedures in Section E.5.4.

…  • If the GTT on the SCCP Called Party Address results in a PC and SSN within the STP’s network, the STP shall verify the ability of the PC and SSN to properly process an XUDT message containing an SCCP ISNI parameter through the use of the “SCCP Application Entity,” defined in Section 5.2.3.3 and in Appendix J, Section J.2. An attribute of this entity shall identify a PC and SSN’s ability to process an XUDT message containing an SCCP ISNI parameter.
If the STP determines that the PC and SSN cannot properly process the message, the message shall fail due to “unauthorized message.” The STP shall perform the SCCP ISNI Error Message Procedures in Section E.5.4.

RE-9 [487] If the Type of ISNI Routing indicator is set to Constrained ISNI Routing and the length of the SCCP ISNI parameter is greater than 2 + 2P, then routing information is present in the parameter and the STP shall perform the following procedures:

1. The first network identifier in the routing information is contained in octets \(2 + 2P\) and \(3 + 2P\), or \([3 + 2P]\) and \([4 + 2P]\). If these two octets identify the STP’s network, the STP shall increment the Counter by one (1) to move the STP’s network identifier from routing information to identification information. The STP performs the following procedures:

   A. If the value of the Counter is not less than seven (7) or the value of the Parameter Length is not greater than 2+2P, then further routing information is not present in the SCCP ISNI parameter (i.e., either the Counter has reached the end of the list, or there are no more identifiers in the routing information).

The STP has completed the SCCP ISNI Message Routing Procedures and shall perform the following procedures to determine a DPC:

   • To determine a DPC for the message, the STP shall perform a GTT on the SCCP Called Party Address as T1.112.4 of GR-246-CORE. defines.

   • If the STP can not perform a GTT, the message shall fail due to a GTT-specific cause. The STP shall perform the SCCP ISNI Error Message Procedures in Section E.5.4.

   • If the GTT on the SCCP Called Party Address results in a PC and SSN within the STP’s network, the STP shall verify the ability of the PC and SSN to properly process an XUDT message containing an SCCP ISNI parameter through the use of the “SCCP Application Entity,” defined in Section 5.2.3.3 and in Appendix J, Section J.2. An attribute of this entity shall

5. Recall that the different brackets indicate different types of SCCP ISNI parameters. The \{\} brackets refer to the octet with the Type 0 SCCP ISNI parameter, and the [\] brackets refer to the octet with the Type 1 SCCP ISNI parameter.

6. If the STP’s network is large, recall that the network is identified by the first octet (i.e., Network Id) only. The second octet can be zeros, the STP’s Cluster Id, or another STP’s Cluster Id (within the large network).
identify a PC and SSN's ability to process an XUDT message containing an SCCP ISNI parameter.

... • If the STP determines that the PC and SSN cannot properly process the message, the message shall fail due to "unauthorized message." The STP shall perform the SCCP ISNI Error Message Procedures in Section E.5.4.

... B. If the value of the Counter is less than seven (7) and the value of the Parameter Length is greater than 2+2P, then routing information is present in the parameter. The STP shall examine the first network identifier in the routing information (i.e., octets \{2 + 2P\} and \{3 + 2P\}, or \{3 + 2P\} and \{4 + 2P\}).

... • If the two octets \{2 + 2P\} and \{3 + 2P\}, or \{3 + 2P\} and \{4 + 2P\}, also identify the STP's network (i.e., this is the second occurrence of the STP's network identifier), the message shall fail due to "redundant SCCP ISNI constrained routing information." The STP shall perform the SCCP ISNI Error Message Procedures as defined in Section E.5.4.

... • If the two octets \{2 + 2P\} and \{3 + 2P\}, or \{3 + 2P\} and \{4 + 2P\}, do not identify the STP's network, the STP shall map the network identifier in the two octets to a DPC.

... • If the two octets \{2 + 2P\} and \{3 + 2P\}, or \{3 + 2P\} and \{4 + 2P\}, do not map to a DPC, the message shall fail due to "message incompatibility." The STP shall perform the SCCP ISNI Error Message Procedures as defined in Section E.5.4.

... The STP has completed the SCCP ISNI Message Routing Procedures.

... 2. If the first network identifier (contained in octets \{2 + 2P\} and \{3 + 2P\}, or \{3 + 2P\} and \{4 + 2P\}) does not identify the STP's network, the STP shall perform the following procedures:

... A. The STP shall map the network identifier in the two octets to a DPC.

... If the network identifier (in octets \{2 + 2P\} and \{3 + 2P\}, or \{3 + 2P\} and \{4 + 2P\}) does not map to a DPC, the message shall fail due to "message incompatibility." The STP shall perform the SCCP ISNI Error Message Procedures as defined in Section E.5.4.

... B. Since the first network identifier (in the routing information) did not identify this STP's network, the STP's network identifier may not be included in the identification information. The STP may need to perform the ISNI identification procedures as follows:
• If the Mark for Identification indicator is set to “Identify Networks,” the STP shall perform the SCCP ISNI Identification Procedures in Section E.5.3.

• If the Mark for Identification indicator is set to “Do Not Identify Networks,” the STP has completed the SCCP ISNI Message Routing Procedures.

Figure E-3 shows the SCCP ISNI Constrained Routing Procedures.
Figure E-3. SCCP ISNI Constrained Routing Procedures
E.5.3 SCCP ISNI Identification Procedures

If the feature in the originating network requests that the SCCP ISNI Identification procedures be performed, then each network that the message traverses will record its network identifier in the SCCP ISNI parameter (if not already present). With the help of the Counter, the STP will check the last network identifier in the identification information carried in the SCCP ISNI parameter. If the last network identifier identifies the STP’s network, the STP does not need to insert its identifier in the parameter. If the last network identifier does not identify the STP’s network, the STP checks the first identifier in the routing information. If the STP’s network identifier is present in the routing information, the STP moves its identifier to the identification information by incrementing the Counter. Otherwise, the STP will insert its network identifier by shifting any routing information down by two octets and inserting its identifier in the two empty octets as part of the identification information.

RE-10 [488] If the message is an XUDT message and the Mark for Identification indicator is set to “Identify Networks,” and the value of the Counter is zero (i.e., P=0), then identification information is not present in the parameter. The STP shall perform the procedures below (third requirement) to insert an identifier.

RE-11 [489] If the message is an XUDT message and the Mark for Identification indicator is set to “Identify Networks,” and the value of the Counter is not zero, then identification information is present in the parameter. The STP shall examine the last network identifier in the identification information (i.e., octets [2P] and [1+2P], or [1+2P] and [2+2P]), and perform the following procedures:

… • If the octets [2P] and [1+2P], or [1+2P] and [2+2P], identify the STP’s network, the STP shall not perform the procedures below to insert an identifier.

… • If the octets [2P] and [1+2P], or [1+2P] and [2+2P], do not identify the STP’s network, the STP shall insert its network identifier as described in the next requirement.

RE-12 [490] If the previous requirements identified the need to insert the STP’s network identifier into the SCCP ISNI parameter, the STP shall perform the following procedures to insert an identifier:

… • If the length of the parameter, indicated by the Parameter Length field, is greater than fourteen, then the parameter already contains the maximum number of network identifiers. The message shall fail due to the inability to perform SCCP ISNI identification. The STP shall
perform the SCCP ISNI Error Message Procedures as defined in Section E.5.4.

… • If the length of the parameter, indicated by the Parameter Length field, is less than fourteen but greater than \(2+2P\), the STP shall shift the information after octet \(1+2P\), or \([2+2P]\), down by two octets.\(^7\)

… • The STP shall place the STP’s network identifier in octets \(2+2P\) and \(3+2P\), or \([3+2P]\) and \([4+2P]\).\(^13\) The STP shall use both its network code and non-zero cluster code as the STP’s network identifier.

… • The STP shall increment the value in the Parameter Length field by two and the value of the Counter by one.

… The STP has completed the SCCP ISNI Message Routing Procedures.

RE-13 [491] If the STP has not determined a DPC for the message via the SCCP ISNI Network Specific or Constrained Routing Procedures, the STP shall perform a GTT on the SCCP Called Party Address, as T1.112.4 of GR-246-CORE defines, to determine a DPC, and perform the following procedures:

… • If the STP can not perform a GTT, the message shall fail due to a GTT-specific cause. The STP shall perform the SCCP ISNI Error Message Procedures in Section E.5.4.

… • If the GTT on the SCCP Called Party Address results in a PC and SSN within the STP’s network, the STP shall verify the ability of the PC and SSN to properly process an XUDT message containing an SCCP ISNI parameter through the use of the “Node Application Entity,” defined in Section 5.2.3.3 and in Appendix J, Section J.2. An attribute of this entity shall identify a PC and SSN’s ability to process an XUDT message containing an SCCP ISNI parameter.

… • If the STP determines that the PC and SSN cannot properly process the message, the message shall fail due to “unauthorized message.” The STP shall perform the SCCP ISNI Error Message Procedures in Section E.5.4.

Figure E-4 shows the SCCP ISNI Identification Procedures.

---

\(^7\) That is, information in octet \(3+2P\) is moved to octet \(5+2P\).
Figure E-4. SCCP ISNI Identification Procedures
E.5.4 SCCP ISNI Error Message Procedures

When an XUDT message containing the SCCP ISNI parameter cannot be transferred to its destination, the message return function will be initiated, if requested by the originating SEP. The purpose of the message return function is to return an Extended Unitdata Service (XUDTS) message indicating that a message has encountered routing failure and cannot be delivered to its final destination. The procedure may be initiated, for example, as a result of insufficient translation information or the inaccessibility of a subsystem or point code. The additional SCCP ISNI-specific routing failures include the redundant routing information and the inability to perform SCCP ISNI Constrained Routing or Identification.

E.5.4.1 Procedures for Deriving the XUDTS Message

RE-14 If the XUDT message containing an SCCP ISNI parameter cannot be transferred to its destination, the STP shall perform the message return procedures described in Section T1.112.4 of GR-246-CORE.

RE-15 If the message return procedures determine that an XUDTS message shall be sent by the STP, the STP shall code the XUDTS message as shown in Section T1.112.3 of GR-246-CORE with the following additional SCCP ISNI-specific information:

A. The coding of the SCCP ISNI-specific return causes are as follows:

\[
\begin{array}{c}
\text{bits} \\
\text{hgfedcba}
\end{array}
\]

\[
\begin{array}{c}
11111110 \text{ Unable to perform SCCP ISNI Identification} \\
11111101 \text{ Redundant SCCP ISNI Constrained Routing Information} \\
11111100 \text{ Unable to perform SCCP ISNI Constrained Routing} \\
11110111 \text{ Message Incompatibility} \\
11110101 \text{ Unauthorized Message} \\
11110011 \text{ Invalid SCCP ISNI Routing Request}
\end{array}
\]

B. The XUDTS message shall contain the SCCP ISNI parameter as possibly modified by the SCCP ISNI Routing and/or SCCP ISNI Identification Procedures. The STP shall not modify the SCCP ISNI parameter in deriving the XUDTS message.

---

8. As the STP performs the SCCP ISNI Procedures, the STP may increment the values of the Counter or the Parameter Length fields, or may insert additional identification information. The SCCP ISNI parameter in the XUDTS message will reflect any of these changes from the SCCP ISNI parameter in the XUDT message.
If the STP has received an XUDT message with an SCCP ISNI parameter that involves performing the SCCP ISNI Message Routing Procedures, the STP may be required to create an XUDTS message with a return cause indicating the reason for message failure.

RE-16 [494] The STP shall select an appropriate return cause for an XUDTS message corresponding to the following guidelines:

- If the message involves performing GTT on the SCCP Called Party Address, as T1.112.4 of GR-246-CORE defines, to determine a DPC, but the GTT procedures fail, the return cause should indicate either “no translation for an address of such nature” or “no translation for such address” as Section 4.3.3.1 describes.

- If the message involves performing a GTT on the SCCP Called Party Address, and the STP determines that the PC and SSN (resulting from the GTT) cannot process a message containing the SCCP ISNI parameter, the return cause should indicate “unauthorized message.”

- If the message involves performing SCCP ISNI Network Specific procedures, but the ICN information in CIC format does not map to ICN information in SS7 format, the return cause should indicate “invalid SCCP ISNI routing request.”

- If the message involves performing SCCP ISNI Network Specific procedures, but the ICN information is not the Null ICN Identity when the Network Specific indicator is set to “10,” the return cause should indicate “invalid SCCP ISNI routing request.”

- If the message involves performing SCCP ISNI Identification procedures, but the STP is unable to perform identification because the SCCP ISNI parameter already contains the maximum number of identifiers (indicated by the parameter length greater than fourteen), the return cause should indicate “unable to perform SCCP ISNI identification.”

- If the message involves performing SCCP ISNI Constrained Routing procedures, and the STP’s network identifier appears in the SCCP ISNI parameter as two consecutive identifiers, the return cause should indicate “redundant SCCP ISNI constrained routing information.”

- If the message involves performing SCCP ISNI message routing procedures, but the Type of ISNI Routing indicator is set to Suggested
ISNI Routing or Reserved, the return cause should indicate “invalid SCCP ISNI routing request.”

… • If the message involves performing SCCP ISNI Constrained Routing procedures, but the network identifier in the SCCP ISNI parameter does not map to a DPC, the return cause should indicate “message incompatibility.”

E.5.4.2 SCCP ISNI Error Message Routing Procedures

The SCCP ISNI capability requires special procedures for routing the XUDTS messages. Usually, if a UDT message cannot be transferred to its destination, the UDTS message is routed on point code and SSN to the originator of the UDT message. However, use of the SCCP ISNI parameter requires that the XUDTS message be routed on global title to the originator of the XUDT message. It should be noted that the originator of the XUDT message codes the Calling Party Address of the XUDT message with translation type = “4”, global title address = originating point code, and subsystem number = appropriate value for the sending application. In addition, the Routing Indicator is set to “route on global title” rather than “route on PC/SSN.” As described in T1.112.4 of GR-246-CORE, translation type 4 serves as an indication that the global title address field already contains the point code and subsystem number to be used in routing the message. If the XUDT message cannot be transferred to its destination, the Calling Party Address of the XUDT message becomes the SCCP Called Party Address of the XUDTS message.

Upon receipt of an XUDTS message with an SCCP ISNI parameter, the STP uses the available routing information in the SCCP ISNI parameter to determine a DPC for the message. The actions at the STP differ from the SCCP ISNI Constrained Routing Procedures in Section E.5.2 in that the Counter is decremented rather than incremented. If routing information is not available, the STP performs a global title translation on the SCCP Called Party Address.

The STP performs the following procedures to determine a DPC and forward the XUDTS message to the originator of the XUDT message.

RE-17 If the STP receives or initiates an XUDTS message containing the SCCP ISNI parameter, the STP shall perform the SCCP ISNI Error Message Routing Procedures as follows:

… 1. Regardless of the setting of the Mark for Identification indicator, the STP shall not perform any SCCP ISNI Identification Procedures.

… 2. If the Type of ISNI Routing is not set to Constrained ISNI Routing, the STP shall route based on the SCCP Called Party Address as described in T1.112.4 of GR-246-CORE.
3. If the Type of ISNI Routing is set to Constrained ISNI Routing, the STP shall perform the following procedures:

A. If the value of the Counter is zero, then routing information is not present in the parameter and the STP shall route based on the SCCP Called Party Address as described in T1.112.4 of GR-246-CORE.

B. If the value of the Counter is not zero then routing information is present in the SCCP ISNI parameter. If the contents of octets \(2P\) and \(1+2P\), or \(1+2P\) and \(2+2P\), identify the STP’s network, the STP shall decrement the Counter.

C. If the value of the Counter is now zero, then the routing information has been exhausted in the parameter. The STP shall route based on the SCCP Called Party Address as described in T1.112.4 of GR-246-CORE.

D. If the value of the Counter is not zero and the contents of octets \(2P\) and \(1+2P\), or \(1+2P\) and \(2+2P\), do not identify the STP’s network, the STP shall map the network identifier in the two octets to a DPC.

E. If the value of the Counter is not zero and the contents of octets \(2P\) and \(1+2P\), or \(1+2P\) and \(2+2P\), identify the STP’s network, the message shall fail due to redundant routing information. The STP shall discard the message.

F. If the network identifier in the two octets does not map to a DPC, the STP shall discard the message.

Figure E-5 shows the SCCP ISNI Error Message Routing Procedures.
Figure E-5. SCCP ISNI Error Message Routing Procedures

- Is the Type of ISNI Routing set to Constrained ISNI Routing?
  - Yes: Proceed to the next step
  - No: Is the value of the Counter set to zero (0)?
    - Yes: Decrement the value of the Counter by one (1)
    - No: Map identifier in octets {2P} and {1+2P}, or [1+2P] and [2+2P], to a DPC

- Is the value of the Counter set to zero (0)?
  - Yes: Error
  - No: Proceed to the next step

- Do the octets {2P} and {1+2P}, or [1+2P] and [2+2P], identify this network?
  - Yes: SCCP ISNI Error Message Routing Procedures complete
  - No: Perform SCCP GTT Procedures
E.6 Examples of SCCP ISNI Parameter Coding

The following two tables are examples of the formatting and coding of the Type 1 SCCP ISNI parameter. The parameters only include one network identifier in the Network Identifier Field of the parameter. In Table E-2, the network identifier is in CIC format, and in Table E-3, the network identifier is the Null ICN Identity.

**Table E-2. Example of the SCCP ISNI Parameter with CICs**

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
<th>g</th>
<th>h</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter Type</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Parameter Length</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Routing Control Indicator</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Routing Control Extension</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Network Identifier Field</td>
<td>2nd CIC digit</td>
<td>1st CIC digit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4th CIC digit</td>
<td>3rd CIC digit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note that the “1st CIC digit” as shown above is the most significant digit of the four digit CIC. For CICs 000 through 999, the “1st CIC digit” is coded as zero (0).

Table E-3 shows the format and coding of the SCCP ISNI parameter with the Null ICN Identity. Recall that the Null ICN Identity is two octets of zeros that serve as a placeholder for the true ICN identity resulting from the GTT.

**Table E-3. Example of the SCCP ISNI Parameter with the Null ICN Identity**

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
<th>g</th>
<th>h</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter Type</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Parameter Length</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Routing Control Indicator</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Routing Control Extension</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Network Identifier Field</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
E.7 SCCP ISNI Operations Requirements

E.7.1 STP Provisioning Requirements

This section defines a generic view of SCCP ISNI provisioning data which will be used to assign, change, retrieve, and delete data which are required to support the procedures described in Section E.5.

The SCCP ISNI memory administration requirements are described in terms of the following:

- Users’ View of SCCP ISNI Provisioning Data Elements (Section E.7.1.1)
- Users’ View of Data Operations [i.e., the commands or transactions to be applied to those elements] (Section E.7.1.2)
- SCCP ISNI Data Base Management Functions [i.e., the data base administration functions for the SCCP ISNI data] Section E.7.1.3.

E.7.1.1 User’s View of SCCP ISNI Provisioning Data

The information presented in this section is based on the terminology associated with entity set/relationship models for relational data bases. The information presented in this section shows how the SCCP ISNI provisioning data in the STP logically and functionally appears to the provisioning user.

The users’ view of SCCP ISNI provisioning data will be defined in terms of entities, entity sets, and attributes.

A detailed description of the entity sets and their attributes is provided below. Each entity set description provides a table format of the entity set and its attributes. The sample tables are for illustrative purposes only. Implementation of the entity sets is not restricted to the tables as shown. These tables should not be interpreted as requirements.

RE-18 [496] The following two entity sets shall be provisioned at the STP:

A. CIC/ICN Identification Entity Set

The CIC/ICN Identification entity set (CIC/ICN-ID-TBL) identifies an ICN routing identifier in SS7 format based on an ICN routing identifier in CIC format.

ATTRIBUTES:

CIC/ICN Routing Identifier - numeric(4), fixed length; the ICN routing identifier in CIC format that will be used to route the
message in the CCS network. Valid CIC/ICN routing identifiers are 0000 through 9999.

*ICN Routing Network Identifier* - numeric(3), fixed length; identifies the network identifier (NI) of the ICN routing identifier which will be used to route the message in the CCS network. This attribute is the base-10 (decimal) representation of the 1-octet binary field used in the SS7 protocol to identify the network identifier for signaling points. Valid NIs are 001 through 255.

*ICN Routing Network Cluster* - numeric(3), fixed length; identifies the network cluster (NC) of the ICN routing identifier which will be used to route the message in the CCS network. This attribute is the base-10 (decimal) representation of the 1-octet binary field used in the SS7 protocol to identify the network cluster for signaling points. Valid NCs are 000 through 255.

**KEY ATTRIBUTES:** CIC/ICN Routing Identifier.

---

**Table 1. Table A. CIC/ICN Identification (CIC/ICN-ID-TBL)**

<table>
<thead>
<tr>
<th>CIC/ICN Routing Identifier</th>
<th>ICN Routing Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>num(4)</td>
<td></td>
</tr>
<tr>
<td>ICN Routing NI</td>
<td>num(3)</td>
</tr>
<tr>
<td>ICN Routing NC</td>
<td>num(3)</td>
</tr>
</tbody>
</table>

---

**B. ICN/DPC Identification Entity Set**

The ICN/DPC Identification entity set (ICN/DPC-ID-TBL) identifies a routing label Destination Point Code (DPC) based on the ICN routing identifier defined in SS7 format.

**ATTRIBUTES:**

*ICN Routing Network Identifier* - numeric(3), fixed length; identifies the network identifier (NI) of the ICN routing identifier which will be used to route the message in the CCS network. This attribute is the base-10 (decimal) representation of the 1-octet binary field used in the SS7 protocol to identify the network identifier for signaling points. Valid NIs are 001 through 255.

*ICN Routing Network Cluster* - numeric(3), fixed length; identifies the network cluster (NC) of the ICN routing identifier which will be used to route the message in the CCS network. This attribute is the base-10 (decimal) representation of the 1-octet binary field used in the SS7 protocol to identify the network cluster for signaling points. Valid NCs are 000 through 255.
binary field used in the SS7 protocol to identify the network cluster for signaling points. Valid NCs are 000 through 255.

*Network Identifier* - numeric(3), fixed length; identifies the network to which the message should be routed. This attribute is the base-10 (decimal) representation of the 1-octet binary field used in the SS7 protocol to identify the network identifier for signaling points. Valid NIs are 001 through 255 or null. If a null value is specified, a null value must be specified for the Network Cluster and Network Cluster Member and an entity with the same ICN Routing NI and NC may not exist. If a null value is not specified, a null value may not be specified for the Network Cluster and Network Cluster Member.

*Network Cluster* - numeric(3), fixed length; identifies the cluster of signaling points within the network to which the message should be routed. This attribute is the base-10 (decimal) representation of the 1-octet binary field used in the SS7 protocol to identify the network cluster. Valid NCs are 000 through 255 or null. If a null value is specified, a null value must be specified for the Network Identifier and Network Cluster Member and an entity with the same ICN Routing NI and NC may not exist. If a null value is not specified, a null value may not be specified for the Network Identifier and Network Cluster Member.

*Network Cluster Member* - numeric(3), fixed length; identifies the specific signaling point within a network cluster in the network to which the message should be routed. This attribute is the base-10 (decimal) representation of the 1-octet binary field used in the SS7 protocol to identify the network cluster. Valid NCMs are 000 through 255 or null. If a null value is specified, a null value must be specified for the Network Identifier and Network Cluster and an entity with the same ICN Routing NI and NC may not exist. If a null value is not specified, a null value may not be specified for the Network Identifier and Network Cluster.

*Relative Cost* - numeric(2), fixed length; the weighting factor applied to the ICN Routing Identifier-routing label DPC object. The costs will be assigned values from 00 to 99, representing the most desirable to the least desirable, respectively. Objects of equal desirability are assigned equal costs. In general, if there are 2 or more routing label DPCs (i.e., network identifier, network cluster, and network cluster member) defined for a given ICN Routing Identifier (i.e., ICN routing network identifier and ICN routing network cluster), the routing label DPC with the lowest relative cost should be selected. If the selected routing label DPC is
unavailable (i.e., inaccessible), the routing label DPC with the next lowest cost should be selected. If there are 2 or more available routing label DPCs with the same relative cost value, a routing label DPC should be selected in such a way that, on average, the selection of a routing label DPC for a given ICN routing identifier is shared equally between these DPCs. A relative cost value may not be specified if a null value is specified for the NI, NC, and NCM of the DPC.

... KEY ATTRIBUTES: ICN Routing Network Identifier, ICN Routing Network Cluster, Network Identifier, Network Cluster, and Network Cluster Member.

... Table 2. Table B. ICN/DPC Identification (ICN/DPC-ID-TBL)

<table>
<thead>
<tr>
<th>ICN Routing Identifier</th>
<th>Routing Label DPC</th>
<th>Relative Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>NI num(3)</td>
<td>NC num(3)</td>
<td></td>
</tr>
<tr>
<td>NI num(3)</td>
<td>NC num(3)</td>
<td></td>
</tr>
<tr>
<td>NI num(3)</td>
<td>NC num(3)</td>
<td>NCM num(3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>num(2)</td>
</tr>
</tbody>
</table>

E.7.1.2 Estimated Number of Provisioned Data Entries

The estimated maximum number of provisioned data entries for the CIC/ICN Identification entity set is 1000. This estimate is based on the fact that presently the CIC codes are 3 digits and thus the number of CICs is at the most 1000. Although the CIC format will be expanded to 4 digits in the future, not all CICs are expected to require a provisioned data entry.

In the absence of the relative cost parameter, the maximum number of provisioned data entries for the ICN/DPC Identification entity set will be the same as for the CIC/ICN Identification entity set. (Note that the same DPC may be entered for multiple ICNs.) If the relative cost parameter is present, multiple DPCs may be entered for the same ICN. Conservatively, each ICN may require two entries of differing DPCs. Thus, the maximum number of provisioned data entries for the ICN/DPC Identification entity set will be twice that of the CIC/ICN Identification entity set, i.e., 2000.

E.7.1.3 Users’ View of Data Operations

The STPs are required to process commands which may be used to add and delete entities from the SCCP ISNI provisioning entity sets and modify their attributes. These are referred to as recent change (RC) commands. The STPs are also required to process commands
which are used to review the contents of the SCCP ISNI entity sets. These are referred to as verify (V) commands. Following are the RC&V command actions that are required to support the procedures described in Section E.5.

RE-19 [497] The STP shall permit the following RC&V command actions to support the procedures described in Section E.5:

... • Add a CIC/ICN Routing Identifier and ICN Routing Identifier to the CIC/ICN Identification Entity Set
... • Delete a CIC/ICN Routing Identifier and ICN Routing Identifier from the CIC/ICN Identification Entity Set
... • Change an ICN Routing Identifier for a given CIC/ICN Routing Identifier in the CIC/ICN Identification Entity Set
... • Verify a CIC/ICN Routing Identifier and ICN Routing Identifier in the CIC/ICN Identification Entity Set
... • Add an ICN Routing Identifier, Routing Label DPC, and Relative Cost to the ICN/DPC Identification Entity Set
... • Delete an ICN Routing Identifier, Routing Label DPC, and Relative Cost from the ICN/DPC Identification Entity Set
... • Change the Relative Cost for a given ICN Routing Identifier and Routing Label DPC in the ICN/DPC Identification Entity Set
... • Verify an ICN Routing Identifier, Routing Label DPC, and Relative Cost in the ICN/DPC Identification Entity Set.

E.7.1.4 Data Base Management Functions

RE-20 [498] The SCCP ISNI provisioning entity sets shall be supported with the data base management functions described in the OTGR Section 2.1: Memory Administration.

E.7.2 STP Performance Management

RE-21 [499] The STPs supporting the procedures in Section E.5 shall provide sufficient measurement data to keep CCS network personnel and their supporting OSs informed as to the processing activities regarding the procedures in Section E.5.
E.7.2.1 Measurement Requirements

The information presented in this section identifies the data that should be collected by the STP and reported to CCS network personnel to support the procedures described in Section E.5.

RE-22 [500] The STP shall collect SCCP ISNI measurements according to the generic requirements provided in the OTGR: Measurements and Data Generation, GR-478-CORE.

RE-23 [501] The STP shall report each measurement to the appropriate CCS network-related OSs and local craft interfaces.

E.7.2.1.1 System Total Measurements

RE-24 [502] The STP shall accumulate the following measurements on a per-STP basis (i.e., system total) according to the indicated accumulation intervals:

1. **MSUs Discarded: SCCP ISNI Processing Error (5,30,d)** - The number of MSUs discarded due to an SCCP ISNI message processing error.

2. **SCCP ISNI Process Incomplete: Invalid SCCP ISNI Routing Request (d)** - The number of times the SCCP ISNI process could not be completed because routing indicates “Suggested ISNI Routing” or “Reserved,” or because the network specific indicator is set to “Reserved”, or because an ICN routing identifier in CIC format could not be translated to SS7 format (e.g., a CIC/ICN Identification translation error occurred), or because the ICN information is not the Null ICN Identity when the Network Specific indicator is set to “10.”

3. **SCCP ISNI Process Incomplete: Unauthorized Message (d)** - The number of times the SCCP ISNI process could not be completed because the PC and SSN (resulting from a GTT) cannot process a message containing the SCCP ISNI parameter.

4. **SCCP ISNI Process Incomplete: Message Incompatibility (d)** - The number of times the SCCP ISNI process could not be completed because the network identifier (in SS7 format) does not map to a DPC (e.g., an ICN/DPC Identification translation error occurred).

5. **SCCP ISNI Process Incomplete: Non-ISNI Equipped Node (d)** - The number of times the SCCP ISNI process could not be completed because the network identifier (in SS7 format) maps to a non-ISNI...
equipped CCS node (e.g., an ICN/DPC translation results in a null DPC).

6. **SCCP ISNI Process Incomplete: Redundant SCCP ISNI Constrained Routing Information (d)** - The number of times the SCCP ISNI process could not be completed due to redundant routing information.

7. **SCCP ISNI Process Incomplete: Unable to Perform ISNI Identification (d)** - The number of times the SCCP ISNI process could not complete ISNI Identification (e.g., the SCCP ISNI Parameter length exceeds 14).

8. **SS7 Translations (30)** - The number of MSUs for which the STP translates the ICN routing identifier (in CIC format) to an ICN routing identifier in SS7 format.

9. **ICN Translations (30)** - The number of MSUs for which the STP translates the ICN routing identifier in SS7 format to a routing label DPC.

10. **Routing Indicates “Suggested SCCP ISNI Routing” or “Reserved” (30)** - The number of MSUs for which routing indicates “Suggested ISNI Routing” or “Reserved.”

11. **Routing Indicates “Constrained ISNI Routing” (30)** - The number of MSUs for which routing indicates “Constrained ISNI Routing.”

12. **Routing Indicates “Neither Constrained Nor Suggested ISNI Routing” (30)** - The number of MSUs for which routing indicates “Neither Constrained Nor Suggested ISNI Routing”.

13. **SCCP ISNI Identification Performed (30)** - The number of MSUs for which SCCP ISNI identification is performed.

**E.7.2.2 Event Reporting**

The information presented in this section identifies the events which should be reported by STPs to CCS network personnel to support the procedures described in Section E.5. The events described in this section should be provided to CCS network-related OSs and maintenance local craft interfaces immediately as they occur according to the standard message format presented in the OTGR Section 12.3: Network Maintenance: Network Element and Transport Surveillance Messages.

**RE-25 [503]** The STP shall report events to CCS network personnel according to the standard output message syntax format described in the OTGR:

RE-26 [504] The STP shall report events to the appropriate CCS network-related OSs and local craft interfaces.

E.7.2.2.1 Event Report Content

RE-27 [505] All event notifications required to support the procedures in Section E.5 shall contain the following information:

- Event ID - the specific trouble reported or detected by the STP
- Time Stamp - the actual time when the event occurred to the nearest second
- Node ID - the CLLI or PC for the STP at which the event to be reported occurred
- Sequence Number - a unique, ordered number associated with each event notification used to determine when messages from a particular STP are missing
- Event Severity - the severity of the event (e.g., critical, major, or minor)
- Detailed Message Information - detailed message information regarding the TCAP message associated with each event notification. Detailed message information may include the following, as appropriate and as available at the time the event notification is generated: Signaling Information Octet (SIO) data (e.g., the Service Indicator and Message Priority) and Signaling Information Field (SIF) data (e.g., the Routing Label OPC and DPC, Message Type, Protocol Class, SCCP Called/Calling Party Address information, SCCP ISNI Parameter information, and TCAP message information).

E.7.2.2.2 Event Report Control Capability

RE-28 [506] The STP shall provide an event notification “throttling” capability which will allow CCS network personnel to suppress or control the number of each individual event notifications which may be reported in a user-specified period of time (e.g., allow no more than ‘n’ events in ‘m’ minutes).


E.7.2.2.3  Event Report Types

The following event notifications are specific to an STP supporting the procedures in Section E.5:

**RE-29** [507] All STP event notifications for the SCCP ISNI capability shall have an event severity of “critical.”

**RE-30** [508] The following events shall be reported to CCS network personnel when they occur:

1. ISNI Message Handling - Incomplete - Error Message Handling Procedures Invoked

   This event notification is reported when the STP cannot complete the processing of a message that requires ISNI-related processing and the message indicates an XUDTS message should be created and routed by the STP (i.e., bits 5 through 8 of the protocol class parameter field indicate “return message on error”). This event notification will include one of the following error descriptions:

   - Invalid SCCP ISNI Routing Request (e.g., routing indicates “Suggested ISNI Routing” or “Reserved”, or the network specific indicator is set to “Reserved”, or an ICN routing identifier in CIC format could not be translated to SS7 format), or the ICN information is not the Null ICN Identity when the Network Specific indicator is set to “10”

   - Unauthorized Message (e.g., the PC and SSN resulting from a GTT cannot process an XUDT message containing an SCCP ISNI Parameter)

   - Message Incompatibility (e.g., a routing label DPC could not be determined for the ICN routing identifier in SS7 format)

   - Redundant SCCP ISNI Constrained Routing

   - Unable to Perform ISNI Identification (e.g., the SCCP ISNI Parameter length exceeds 14) 9

2. ISNI Message Handling - Incomplete - Message Discarded

   This event notification is reported when the STP cannot complete the processing of an XUDT message that requires ISNI-related processing

---

9. This error condition occurs when seven routing and/or identification network identifiers already exist in the SCCP ISNI parameter. The ISNI Identification process cannot be performed as requested since the maximum number of routing and/or identification network identifiers that can exist in the parameter is 7 (i.e., another network identifier cannot be added to the parameter).
and the XUDT message indicates that an XUDTS message should not be created and routed by the STP (i.e., bits 5 through 8 of the protocol class parameter field indicate “discard message on error”).

3. ISNI Error Message Handling - Incomplete - Message Discarded

This event notification is reported when the STP cannot complete the ISNI Error Message Handling procedures that are invoked when an XUDTS message encounters an error during ISNI-related processing (e.g., an error occurs when the STP initiates or routes an XUDTS message).

E.8 SCCP ISNI Performance Requirements

Section 8.2 describes the STP performance requirements for STP transport time, including the SCCP ISNI procedures.

RE-31 [509] SCCP ISNI shall not affect the STP node processing time beyond the requirements that Section 8.2 presents.
Appendix F: Translation Type Mapping Function

F.1 Introduction

The type of global title processing required at an STP is determined by the translation type in the SCCP Called Party Address. (See Section 4.3.3.3 for SCCP routing controls for global title translation.) The translation type values are used for intra as well as internetwork messaging. Standardized translation type code values for internetwork applications are used for SS7 messages that cross network boundaries, and those values may be different from the translation type values used within any particular network. This fact has created a need for a mapping capability to associate the internetwork translation type value with the value currently being provisioned within the network.

This appendix specifies procedures and requirements for the translation type mapping function at the STP. The organization of this section follows the organization of the STP requirements in the ordering of relevant sections. Section F.2 provides definitions found throughout this appendix. Section F.3 provides the translation type mapping procedures and relevant generic requirements. Section F.4 describes additional operations requirements, including provisioning and administration capabilities, needed at the STP to support the translation type mapping function. Section F.5 discusses performance considerations for the translation type mapping function.

F.2 Definition of Terms

The following terms are used throughout Appendix F:

- Incoming gateway link set - A link set designated as one in which messages are being received from another signaling network.

- Outgoing gateway link set - A link set designated as one in which messages are being transmitted to another signaling network.

- Existing translation type - The translation type value included in the Called Party Address of a Unitdata (UDT) or Extended Unitdata (XUDT) message on an incoming or outgoing gateway link set which will be used for the translation type mapping function.

- Mapped translation type - The translation type value provisioned in a translation type mapping data set which is associated with the existing translation type value and will be used to replace the existing translation type value.

- Translation Type Mapping Function - The process of examining the existing translation type value and replacing it with an associated translation type value, if the existing value is included in the provisioned data set.
F.3  The Translation Type Mapping Function

This section describes the overall actions of the STP when the STP is receiving or transmitting a UDT or XUDT message and translation type mapping is required.

F.3.1  Scope of Activation

Messages received across network boundaries as well as messages to be sent across network boundaries may need to be examined for translation type values. Therefore, any gateway link set may be designated as a link set requiring the translation type mapping function.

RF-1  [510] The translation type mapping function shall be designated on a per-gateway link set basis.

F.3.2  SCCP UDT and XUDT Messages

The translation type mapping function applies to all UDT and XUDT messages received or transmitted on gateway link sets designated for translation type mapping, regardless of whether global title translation is required for the message or not. The Called Party Address field in these messages includes the translation type value which is to be examined for the mapping function. It is assumed that UDTS messages are MTP-routed and need not be examined. Furthermore, an XUDTS message will either be MTP routed or will use one translation type value (i.e., “4”) indicating global title to point code translation and should not be mapped.

RF-2  [511] The translation type mapping function shall be applied to all SCCP UDT and XUDT messages transmitted or received on a designated gateway link set provisioned for translation type mapping.

F.3.3  Incoming and Outgoing Messages

It may be desirable to change the value of the translation type on both an incoming gateway link set and outgoing gateway link set basis. Incoming translation type mapping is required to support the acceptance of UDT and XUDT messages that include a different translation type for a requested service. The receiving STP maps the existing translation type to the mapped translation type it uses for the requested service and replaces the value. Outgoing mapping is required to support the transmission of UDT and XUDT messages that require a different translation type for the requested service. The transmitting STP maps the existing translation type to the mapped translation type and replaces the value. If the translation type is not provisioned in the mapping data, no action is taken.
The capability shall exist to provision any gateway link set for incoming mapping, outgoing mapping, or both.

On gateway link sets which are designated for incoming mapping, the translation type value shall be replaced with the mapped translation type value indicated in the incoming gateway link set translation type mapping information.

On gateway link sets which are designated for outgoing mapping, the translation type value shall be replaced with the mapped translation type value indicated in the outgoing gateway link set translation type mapping information.

Gateway screening is performed on incoming SS7 messages that arrive on designated gateway link sets. Most common implementations of internetwork database services require SCCP processing of a global title at the point of entry into a network. (Gateway screening is described in Appendix C.) This process includes screening of the translation type value in the Called Party Address. If a global title translation is required at the gateway STP, additional SCCP screening is required. If a gateway link set is designated as a translation type mapping link set, the following requirements must be met:

On an incoming gateway link set, the translation type mapping function shall occur before global title translation, billing or final SCCP screening.

On an outgoing gateway link set, the translation type mapping function shall occur after global title translation, billing or final SCCP screening.

This section provides the operations requirements associated with the translation type mapping function.

This section defines a generic view of the provisioning data which will used to assign, change, retrieve, and delete data which are required to support the translation type mapping
The translation type mapping memory administration requirements are described in terms of the following:

- User’s View of Translation Type Mapping Provisioning Data Elements (Section F.4.1.1)
- User’s View of Data Operations [i.e., the commands or transactions to be applied to those elements] (Section F.4.1.2)
- Translation Type Mapping Database Functions [i.e., the database administration functions for the translation type Mapping data] (Section F.4.1.3).

F.4.1.1 User’s View of Translation Type Mapping Provisioning Data

The information presented in this section is based on the terminology associated with entity set/relationship models for relational databases. What is presented is how the translation type mapping provisioning data in the STPs logically and functionally appear to the provisioning user.

The users’ view of translation type mapping provisioning data will be defined in terms of entities, relationships, and attributes. (See Section 5.2.3.1 for more detail.)

The translation type mapping relationship has been defined for the generic user view of translation type mapping data. All the attributes defined for the translation type mapping relationship are of fixed length, meaning they must always have the maximum length specified.

This section provides a detailed description of the translation type mapping relationship and its attributes.

RF-8 [517] The following relationship is required to support the translation type mapping capability:

... A. Translation Type Mapping

... The translation type mapping relationship identifies a new translation type for an Signaling System 7 (SS7) message based on the gateway link set on which the message was received (i.e., incoming gateway link set) or will be sent (i.e., outgoing gateway link set), and the SS7 message’s translation type prior to translation type mapping.

... ATTRIBUTES:

... Gateway Link Set Name - alphanumeric (8), fixed length; the unique network identifier for the gateway link set. The gateway link set name is used to uniquely reference gateway link sets in the network. It is represented by a COMMON LANGUAGE™ code called a link set serial number, also referred to as a 1-1-6 Code or 2-6 Code. It is a unique
designation comprised of one alphabetic character concatenated with one
alphanumeric character and six numeric characters (1-1-6 Code) or two
alphabetic characters concatenated with six numeric characters (2-6
Code).

…

Incoming/Outgoing Indicator - alphabetic (1), fixed length; used by the
STP to indicate whether the translation type mapping data provisioned for
the gateway link set is for SS7 messages received on the link set, or sent
on the link set. Allowable Incoming/Outgoing (I/O) Indicator values are: I
(incoming) and O (outgoing).

…

Existing SS7 Message Translation Type - numeric (3), fixed length; the
identification of the type of allowed global title translation in the SS7
message prior to translation type mapping. This attribute is the decimal
representation of the 1-octet binary field used by the SS7 protocol to
identify the translation type. Allowable Existing SS7 Message Translation
Type values are: 001 through 254.

…

Mapped SS7 Message Translation Type - numeric (3), fixed length; the
identification of the type of allowed global title translation in the SS7
message after translation type mapping. This attribute is the decimal
representation of the 1-octet binary field used by the SS7 protocol to
identify the translation type. Allowable Mapped SS7 Message Translation
Type values are: 001 through 254.

…

KEY ATTRIBUTES: Gateway Link Set Name, Incoming/Outgoing
Indicator, and Existing SS7 Message Translation Type.

F.4.1.2 User’s View of Data Operations

The STP is required to process commands which may be used to add and delete entities
from the translation type mapping entity set and modify its attributes. These are referred to
as recent change commands. The STP is also required to process commands which are used
to review the contents of the translation type mapping entity set. These are referred to as
verify commands. Below are the RC&V command actions defined for the Network
Element (NE) - to - OS interface to support the translation type mapping capability.

RF-9 [518] The following RC&V command actions are required to support the
translation type mapping capability:

…

RECENT CHANGE COMMANDS:

…

• Add a Gateway Link Set Name, Incoming/Outgoing Indicator,
  Existing SS7 Message Translation Type, and Mapped SS7 Message
  Translation Type to the translation type mapping entity set.
… • Delete a Gateway Link Set Name, Incoming/Outgoing Indicator, Existing SS7 Message Translation Type, and Mapped SS7 Message Translation Type from the translation type mapping entity set.

… • Change a Mapped SS7 Message Translation Type for a given Gateway Link Set Name, Incoming/Outgoing Indicator, and Existing SS7 Message Translation Type in the translation type mapping entity set.

… VERIFICATION COMMANDS

… • Verify a Gateway Link Set Name, Incoming/Outgoing Indicator, Existing SS7 Message Translation Type, and Mapped SS7 Message Translation Type in the translation type mapping entity set.

F.4.1.3 Database Management Functions

RF-10 [519] The translation type mapping entity set shall be supported with the database management functions described in the OTGR: Memory Administration.

F.4.2 STP Performance Management

F.4.2.1 Measurement Requirements

RF-11 [520] The translation type mapping-related administration measurements shall be collected according to the general requirements provided in the OTGR: Measurements and Data Generation.

Each subsection below lists the measurements that must be maintained for translation type mapping. The accumulation intervals are indicated in the parenthesis and are represented as described in Section 6.4.1.

F.4.2.1.1 System Total Measurements

RF-12 [521] The following measurement shall be maintained over the indicated accumulation intervals for the STP system:

… Translation Type Mapping Translations Performed (5,30,d) - The total number of Translation Type Mapping translations performed (i.e., a mapped SS7 message translation type was found for the existing SS7 message translation type).
F.4.2.1.2 Translation Type Measurements

RF-13 [522] The following measurement shall be maintained over the indicated accumulation intervals on a per-translation type basis for each Existing SS7 Translation Type provisioned in the Translation Type Mapping entity set:

... Translation Type Mapping Translations Performed (30) - The total number of Translation Type Mapping translations performed (i.e., a mapped SS7 message translation type was found for the existing SS7 message translation type).

F.4.2.1.3 Gateway Link Set Measurements

RF-14 [523] The STP shall provide the following measurements on a per-gateway link set/per translation type basis for each Existing SS7 Translation Type provisioned in the Translation Type Mapping entity set:

... 1. Translation Type Mapping Translation Performed: MSUs Received on the Gateway Link Set (30,d) - The total number of Translation Type Mapping translations performed for Message Signal Units (MSUs) received on the gateway link set (i.e., incoming).

... 2. Translation Type Mapping Translation Performed: MSUs Transmitted on the Gateway Link Set (30,d) - The total number of Translation Type Mapping translations performed for Message Signal Units (MSUs) transmitted on the gateway link set (i.e., outgoing).

F.4.3 Event Reporting

F.4.3.1 Message Tracking Capability

It may be necessary for a Bcc to verify the processing that a message received on a particular gateway link set or transmitted on a particular gateway link set would receive to assist in trouble shooting SS7 messages that use the translation type mapping capability.

RF-15 [524] The STP shall provide the capability for the Bccs to manually verify the global title translation output, the link set selection, and the translation type mapping output for a particular outgoing SS7 message.
**RF-16** [525] The STP shall provide the capability for the Bccs to manually verify the translation type mapping output and the global title translation output for an incoming message on a particular incoming gateway link set.

**F.5 Performance Requirements**

Section 8.2 describes the STP performance requirements for STP transport time, including translation type mapping.

**RF-17** [526] Translation type mapping shall not affect the STP node processing time beyond the requirements that Section 8.2 presents.
Appendix G: Priority Processing of Network Management (NM) Tasks in STPs

Appendix G describes Bellcore’s view of the priority processing of network management tasks in STPs. Network management task priority processing is needed to ensure that critical network management tasks that are required to maintain the integrity of the CCS network are given higher processing priority than non-critical network management tasks. Sections 4.2.4 and 4.3.3 provide specific requirements for network management priority processing. The information described in this appendix is not intended to provide any specific implementation approach. It is intended to serve as a generic model to describe the concept of network management priority processing.

In this GR, a “network management task” refers to processing functions performed by a processor responsible for network management functions in an STP. These tasks are performed either in response to received network management messages from other nodes or on detection of local failures in the STP or its associated facilities (e.g., links, link sets, routes). For example, receipt of a MTP transfer-prohibited (TFP) message prompts the STP to assign a number of different network management processing tasks including processing the incoming TFP, rerouting of traffic to an alternate route, and broadcasting TFPs to adjacent nodes. Section G.3 further describes network management tasks. The term network management is used to refer to all MTP network management and SCCP network management functions defined in T1.111.4 of GR-246-CORE.

G.1 Introduction

Network management tasks are, in general, assigned equal processing priority at the STP and processed in the same sequence that the processor receives them. That is, network management messages are queued in the internal processor buffer and response actions are performed based on the sequence in which they are received. In this concept, a less critical function (such as restoring a newly available signaling route when all traffic has been successfully diverted to the alternate route) is performed first if the triggering event for this function is acknowledged by the processor before the triggering event for a more critical function (such as rerouting of traffic away from a failed route).

Although this processing concept may not have serious impact on the network during normal operation, it may seriously impact the network’s recovery capabilities under large scale failure conditions when the STP must perform several critical network management functions (such as rapidly bringing a large number of links in and out of service or rerouting traffic away from a large number of failed routes). In addition, under this failure scenario, the STP network management processing capacity could be exhausted doing non-critical functions resulting in less real processing time available for more critical functions. The STP network management priority processing capability provides a method to optimize the network management processing under a large scale failure.
The basic concept of priority processing of network management tasks in STPs involves assigning priorities to each network management tasks from a priority range of 0 to 3 based on the criticality of the task. Network management tasks of high priority are processed before any lower priority tasks are processed. Priority processing can be activated on reaching an overload threshold in the network management processor or can remain effective all the time. Lower priority tasks are held in the processor buffers and processed only when no higher priority tasks are waiting to be processed. The lower priority tasks are stored in the buffer for a specific period of time, after which the task can be removed. The STP should be able to verify and update, if required, the status of lower priority tasks in the queue when a higher priority task is scheduled, ensuring that lower priority tasks reflect the current status of the applicable link or route for the affected destination. Figure G-1 shows a conceptual view of the network management priority processing.

Figure G-1. Network Management Priority Processing Conceptual View
The network management priority processing method described in this appendix is based on the following two basic STP capabilities:

- The STP capability of monitoring the occupancy levels of its network management processors and identifying an overload threshold at which priority processing will be activated (this capability is not required if the priority processing remains effective under all conditions)
- The STP’s ability to assign priorities to network management tasks it schedules and to process these tasks based on a preassigned network management task prioritization scheme.

### G.2 Monitoring of NM Processor Occupancy

Monitoring the STP network management processor load is a basic capability of an STP, as Section 5.3.2 defines. The processor load should be monitored continuously to determine the percent processor occupancy and the real-time available for processing of network management tasks at a given time. In conjunction with monitoring the processor occupancy, a processor overload threshold needs to be defined at which the network management processing of the STP would be at risk. The threshold could be determined based on one of the following criteria:

- A level of the processor utilization at which the STP performance objectives for network management message processing will not be met. Section 4 defines the STP performance objectives for network management message processing.
- A level of processor utilization where the stable operating limits of the processor cannot be predicted.

Because processor occupancy threshold depends on several factors, including the STP architecture and the type of processor used, it should be defined by each STP supplier based on the STP design. The target occupancy threshold could be set at 80 to 90% of the processor occupancy. Since activating the priority processing may result in some loss of network capability (e.g., delaying some network management tasks), a higher setting in this range would be appropriate.

### G.3 STP NM Task Prioritization

Prioritizing NM tasks at STPs should be based on the consideration that network management tasks needed to support the primary functionalities of the CCS Network (CCSN) are given the highest priority. At the STP, these functionalities would involve the efficient transport of SS7 messages to the specified destinations without delay and minimizing the potential for message loss. Tasks beyond these functionalities are then assigned lower priorities in the order of their importance in supporting other CCSN
functions. For example, tasks that are required to support efficient network resource utilization are assigned the next priority.

The NM tasks at an STP can be classified into four priority classes within a priority range of 0 to 3, with 3 being the highest priority and 0 being the lowest priority. Each NM task is then assigned a specific priority based on the following criteria:

- **Priority Level 3**: NM tasks that minimize potential for message loss by providing a path for the message traffic during failures. Restoration of traffic for a destination previously made unavailable is an example.

- **Priority Level 2**: NM tasks that ensure efficient CCSN resource (e.g., links, routes) utilization such as restoring traffic to primary routes from alternate routes and performing congestion control tasks.

- **Priority Level 1**: NM tasks that prevent escalation of failure effects to other parts of the network by stopping the flow of traffic from the originating source to the failure point such as notifying other signaling points through the broadcast method that a particular destination or route is prohibited through the STP.

- **Priority Level 0**: NM tasks for maintaining CCSN surveillance and monitoring functions such as performing audit functions to verify the status of routes or signaling points.

The priority levels identified above may each contain a multitude of different tasks from various NM functional groups (i.e., signaling traffic management, signaling route management, signaling link management, and SCCP management). The following sections discuss various STP tasks under each of these functional groups and their relative ranking in terms of their criticality, as the above priority classifications define. Table G-1 (at the end of this appendix) provides detailed guidelines for assigning priorities to specific tasks.

### G.3.1 Signaling Traffic Management (STM) Functions.

STM functions are used to divert signaling traffic from links or routes. These functions are invoked under any one of the following conditions:

- The STP determines that local links or routes are unavailable (failed) or available (restored).
- The STP receives signaling route management messages (TFx and TCx) indicating the unavailability or availability of remote routes.
- The STP receives local management commands for inhibiting or uninhibiting links or if conditions for forced inhibit of links exist.
- The STP detects congestion in the buffer associated with its local links.
Based on the cause of initiation of STM functions, the STP may then perform one or more of the procedures under STM functions. The STP tasks in performing these procedures may vary from simple updating of routing tables with the congestion status of a route-set to conducting complete steps involved in diverting traffic from a failed route. Detailed actions at the STP for each of the procedures are summarized in the following paragraphs.

G.3.1.1 Changeover/Changeback Procedures

When an STP determines that its local links or routes are unavailable for transporting traffic, it performs changeover of traffic carried by the unavailable link to the alternate link. The STP tasks associated with this procedures are as follows:

- Terminate acceptance and transmittal of MSUs on failed link
- Start transmitting Link Status Signal Units (LSSUs) or Fill-in Signal Units (FISUs)
- Determine alternate links
- Update contents of retransmission buffer
- Divert traffic to alternate links
- Update routing tables
- Send traffic contained in the transmit and retransmit buffers.

When the STP recognizes that a previously unavailable primary link is available again, it invokes changeback procedures. The STP tasks associated with this procedures are as follows:

- Determine alternate links
- Divert signaling traffic (stop traffic on the alternate link, send changeback declaration)
- If needed, invoke sequence control and/or time controlled diversion procedures.

G.3.1.2 Forced/Controlled Rerouting Procedures.

When the STP determines the unavailability of remote routes for a particular destination by the receipt of TFP messages, it performs forced rerouting to divert the traffic away from the failed route. The forced rerouting procedure involves the following tasks at the STP:

- Process received TFPs
- Update routing tables
- Stop traffic to concerned destinations
- Store traffic in the forced rerouting buffer
• Determine alternate routes
• Restart traffic on alternate route.

Controlled rerouting procedures are invoked when the STP recognizes that a previously unavailable route is available by receiving a TFA or when a TFR is received indicating that traffic for a remote destination should be sent through an alternate route. The STP tasks involved for this procedure are as follows:

• Update routing tables for received TFAs or TFRs
• Stop traffic on the route over which the TFR is received or on the alternate route if traffic was previously diverted to the alternate route
• Store traffic in the controlled rerouting buffer
• Start traffic on the route made available by the receipt of TFA or on the alternate route in the case of receipt of TFRs.

G.3.1.3 MTP Restart Procedures

MTP restart procedures are invoked at an STP by the management function when the STP becomes available after it remained unavailable for a period of time defined in GR-246-CORE, T1.111.4, Section 9.1. The MTP restart procedures involve coordinated use of STM and Signaling Route Management (SRM) functions. Thus, STP tasks involved in the MTP restart procedures are included within applicable STM and SRM procedures. The MTP restart procedures are invoked under the management function, which ensures that network management functions are controlled and only some of the functions are exercised. The possibility of network management processing overloading under this controlled environment is considered remote.

G.3.1.4 Link Inhibiting/Uninhibiting

Management requests signaling link inhibiting or uninhibiting when it becomes necessary. A signaling link remains inhibited unless it is uninhibited. A signaling link can be forced uninhibited by the signaling routing control if the inhibiting of the link results in a destination becoming unavailable. The STP tasks involved in response to a link inhibiting or uninhibiting command are as follows:

• Check to make sure inhibiting of the link will not result in the destination becoming inaccessible or uninhibiting is possible
• Send inhibited or uninhibited message to the other end
• If acknowledgment is received from the other end, mark the link locally inhibited or uninhibited and start test procedures
• If the link was carrying traffic, initiate changeover or changeback procedures to divert the traffic.

Signaling link uninhibiting procedures are similar to the inhibiting procedures except in the case of forced uninhibiting. Here, after a check is made to determine that the inhibiting of the link makes a destination inaccessible, the STP sends a forced uninhibit link message to the other end, which will then initiate normal uninhibiting procedures.

G.3.1.5 Signaling Traffic Flow Control

Signaling traffic flow control procedures are invoked at the STP when it cannot transfer signaling traffic offered by the user parts due to congestion in the route set for a particular destination. The STP tasks involved in these procedures are as follows:

• Update routing tables with appropriate congestion status of the route set as determined by the congestion status of the received transfer controlled message or by recognizing local signaling link congestion or due to the signaling route set congestion test procedure

• Inform the local users of the congestion status of the route set.

G.3.1.6 Ranking of STM Tasks

As discussed in the previous sections, some STP STM tasks are considered more critical than others. For example, diverting traffic from a failed route using forced rerouting procedures is more critical than restoring traffic from an alternate route to the normal route using controlled rerouting procedures. This is because in the first case, the failure to immediately restore traffic may result in message loss or further escalation of the failure impact, while restoring traffic to the normal route from an alternate route may only avoid the possibility of congestion in the alternate route. Based on this example, the following ranking for NM tasks under the STM functions is derived.

1. Perform critical routing changes.
   • Perform forced rerouting procedures in response to received TFPs or TCPs to divert traffic away from a prohibited route.
   • Perform controlled rerouting for the affected destination only if the destination is marked prohibited on that route (receipt of an TFA).
   • Perform changeover to divert traffic from failed links to alternate links.
   • Perform forced uninhibits when an inhibiting condition results in the isolation of a point code.

2. Perform non-critical routing changes.
• Perform controlled rerouting to divert traffic to an alternate route in response to a received TFR or TCR.
• Perform changeback to normal links from alternate links when a previously failed normal link becomes available.
• Perform link uninhibiting in response to a management uninhibit command.

3. Inform user part about the local link congestion.

4. Perform link inhibiting in response to a management inhibiting command.

G.3.2 Signaling Route Management (SRM) Functions

SRM functions are used to exchange route status information among signaling points, notify other signaling points of changes in the status of routes, and perform network audit functions. The STP tasks involved in carrying out SRM functions include the following:

• Process incoming transfer messages (i.e., TFP, TCP, TFR, TCR, TFA, TCA) and update routing tables accordingly.
• Send a TFP or TCP in response to a received message when it is unable to transfer the message to the given destination.
• Broadcast transfer messages (i.e., TFP, TCP, TFR, TCR, TFA, TCA) to adjacent nodes to notify them of the unavailability or availability of a route for a given destination.
• Initiate signaling route set test messages in response to TFP, TCP, TFR, and TCR.
• Send a TFC message when detecting congestion in the transmit buffer for a route associated with a destination.
• Process (updating of routing tables) received TFC messages.
• Send route-set-congestion-test messages in response to received TFCs.
• Process incoming signaling-route-set-test messages and respond if the route set status has changed.
• Process incoming route-set-congestion-test messages and respond if the congestion status of the affected route set has changed.

Ranking of the STP tasks associated with the SRM function is provided below.

1. Triggering events for critical routing changes.
   • Process incoming TFP and TCP messages and appropriately mark affected routes in the routing table.
• Process incoming TFA and TCA messages and mark routing tables for those routes that were previously marked prohibited or restricted.

• Send TFPs and TCPs by the response method on detecting local link set failures.

2. Triggering events for non-critical routing changes.

• Process incoming TFR and TCR messages and mark affected routes in the routing table.

• Process incoming TFC messages and update routing tables.

• Send TFC messages in response to any message that encountered congestion in its outgoing links.


• Broadcast TFx (TFP, TFR, TFA) and TCx (TCP, TCR, TCA) messages to adjacent nodes to notify routing changes at the STP.

• Network audit
  — Send RSx (RSP, RSR) and RCx (RCP, RCR) messages in response to received TFP, TCP, TFR, and TCR messages.
  — Send RCT messages in response to received TFCs.

• Response to audit messages
  — Respond to received RSx and RCx messages with appropriate TFx or TCx.
  — Respond to RCT messages if the congestion status of the route set has changed.

G.3.3 Signaling Link Management (SLM) Functions

SLM functions are used to control the locally connected signaling links, including the function that allows it to maintain a predetermined number of links in a link set in the event of signaling link failures. The SLM functions can be invoked manually or automatically. In the first case, when a link or link set is brought into service for the first time, the SLM procedures to activate the link are started. In the second case, when a signaling link failure is detected, the SLM procedure is started to either restore the link or deactivate the link. The SLM functions include the following:

• Signaling Link Activation/Restoration/Deactivation

• Signaling Link Set Normal Activation/Emergency Restart.

In this GR, the SLM procedures that are invoked during a failure condition are examined since the activation/deactivation procedures performed during the initial starting are not expected to cause NM overloading. The STP should be able to maintain the required number of links in a link set during a failure by automatically activating links or restoring
failed links so as to minimize further degradation of the remaining good links. Similarly, on detection of the failure of a link or a link set, the STP should be able to deactivate the affected link or link set.

Primary STP actions to perform activation and restoration procedures include initial link alignment and signaling link tests.

Depending on the failure, the SLM tasks in some cases would be highly critical. (For example, in the case of failures of B-links to another pair of STPs that resulted in traffic diversion to C-links. This would require that B-links be brought back to service as soon as they become available using activation/deactivation procedures.) In other cases it may not be that critical. Given the various scenarios, it will be too burdensome on the STP to determine the severity of the failure and then determine if the appropriate SLM procedures need to be invoked. Additionally, since the major tasks in these procedures are generally carried out by the link level processors, the SLM tasks should remain high priority tasks.

Processing signaling link test messages received periodically from an adjacent node, should also be considered a high priority task.

G.3.4 SCCP Management Functions

SCCP management functions provide the STP capability to throttle and reroute traffic in the event of network failures associated with the SCCP message handling. SCCP management procedures are invoked in response to signaling point or route failure or recovery as well as subsystem failure or recovery. SCCP management tasks at the STP primarily include the following:

- Update routing tables (e.g., global title translation tables) based on received point code or subsystem status messages
- Send subsystem-prohibited and subsystem-allowed messages to concerned signaling points
- Send subsystem-status-test messages in response to received SSPs.

The ranking of SCCP management tasks is again built on the fact that performing routing changes in the event of a failure is of primary importance, followed by tasks that notify other nodes of the changes in the routing status. Tasks are thus ranked in the following order:

1. Update global title translation table in response to received SSPs or point code failure. This would involve routing to an alternate node or subsystem.
2. Update global title translation table in response to received SSAs. This will accomplish the restoration of routing to the primary subsystem or point code.
3. Broadcast SSPs and SSAs to concerned signaling points in the event of subsystem failures or restorations.
4. Send subsystem status test messages in response to SSPs.
5. Respond to received subsystem status test messages.

G.4 Priority Assignments for NM Tasks

Table G-1 provides recommended priorities for network management tasks based on the network management task ranking established in Section G.3. Task priorities are assigned within a range of 0 to 3, where 3 is the highest priority.

G.5 NM Task Validation

Important considerations for implementing the priority processing concept is to ensure that lower priority tasks are not lost while waiting to be performed, to ensure that lower priority tasks waiting in the queue at a given time correspond to the current state of the network (e.g., the affected route or destination), and to verify that these tasks have not been invalidated by a recently received higher priority task. Therefore, STPs must include a capability to verify the status of lower priority tasks. For example, when an STP receives a TFP on a route for a given destination, it should assign a high priority task to update the routing table. At the same time, the STP should also be able to verify that there are no lower priority tasks, such as processing a TFR or TFA, queued in the lower priority buffers for the same route and destination. This could occur if the STP was unable to act on these lower priority tasks corresponding to an earlier state of the route for the same destination due to the long queue length of higher priority tasks.

It is envisioned that in a generic processor architecture, when an STP receives a NM message, it invokes a number of NM tasks. It will be the function of the processor to identify the various tasks (or services) that need to be provided. The processor may then assign each task (or service) to separate registers based on the priority of the task. The processor then polls each register, when it is ready to perform the next task, to identify the next task (or service) to be provided. Therefore, when a task is placed in a register, it is necessary that the processor verifies that registers of a lower priority are cleared of tasks that apply for the same destination and are of the same functional category.

Functional relationships among tasks should be established prior to the clearing of lower priority tasks, in addition to ensuring that affected tasks apply for the same destination or route. For example, if a TFC is received followed by a TFR for the same destination, it would be undesirable to remove the lower priority task of processing the TFC when the higher priority TFR processing task is assigned. Table G-2 provides a matrix of tasks that need to be verified or updated, if required, when a given higher priority task is assigned.

In addition, because under extreme processor overloading, the processor may not be able to process lower priority tasks for some period of time, performing lower priority tasks after it has been queued for a long period of time may not be desirable from the network point
of view and would require more buffer space for these tasks. To alleviate this, STPs should provide the capability to remove tasks that have been queued over a specified amount of time. Considering that timers specified in the SS7 protocol and in Section 6 for network management functions are all within the range of milliseconds to seconds, removing tasks after it has been queued for 1 minute would have minimum impact on the network.
### Table G-1. Guidelines for NM Task Priority Assignments at STPs

<table>
<thead>
<tr>
<th>Task Priority</th>
<th>STP Tasks</th>
</tr>
</thead>
</table>
| **Level 3:**  | 1. Process received TFPs and TCPs, update routing tables, and reroute traffic to alternate routes.  
|               | 2. Process received TFAs and TCAs for those destinations that were previously made inaccessible, update routing tables, and reestablish traffic through the affected routes.  
|               | 3. Process received TFAs and TCAs for those destinations for which traffic was previously rerouted to alternate routes, update routing tables, and reroute traffic through newly available route.  
|               | 4. Process received TFRs and TCRs, update routing tables, and reroute traffic through alternate routes.  
|               | 5. Changeover traffic from failed links and update routing tables.  
|               | 6. Forced uninhibit of inhibited link.  
|               | 7. Send TFPs and TCPs by response method.  
|               | 8. Signaling link activation/deactivation/restoration including tasks associated with signaling link tests.  
|               | 9. Update global title translation tables in response to received SSPs or point code unavailability. |
| **Level 2:**  | 1. Changeback traffic to normal links from alternate links.  
|               | 2. Link uninhibiting in response to management command.  
|               | 3. Process received TFCs and update routing tables.  
|               | 4. Send TFCs by the response method when congestion is encountered.  
|               | 5. Update global title translation tables in response to received SSAs. |
| **Level 1:**  | 1. Inform User Parts about the local link congestion.  
|               | 2. Broadcast TFx and TCx to adjacent nodes.  
|               | 3. Broadcast SSPs and SSAs to concerned signaling points. |
| **Level 0:**  | 1. Send route set test messages in response to received TFx or TCx.  
|               | 2. Send route set congestion test messages in response to received TFCs.  
|               | 3. Send SSTs in response to received SSPs.  
|               | 4. Link inhibiting in response to management command.  
|               | 5. Respond to received RSx and RCx with appropriate TFx and TCx.  
|               | 6. Respond to RCT with TFCs.  
|               | 7. Response to SSTs. |
### Table G-2. Validation Matrix For Lower Priority Tasks

<table>
<thead>
<tr>
<th>Priority and Task Assignment</th>
<th>Verify and clear Tasks ††</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Task Number†</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

† Task numbers refer to tasks identified in Table G-1.

†† Task verification should apply when the lower priority task corresponds to the same affected destination as indicated in the higher priority task.
Appendix H: Guidelines to Determine GTT Table Sizes

H.1 Introduction

Accurate estimation of the memory capacity required for Global Title Translation (GTT) tables in the Bcc STP has been difficult in the past. To help increase STP supplier and Bcc understanding of the memory capacity requirements for GTT tables, this appendix provides worst case estimates of the number of GTT table entries required for several services. The services included are CLASS features (specifically Automatic Recall [AR], Automatic Callback [AC], and Screening List Editing [SLE]), Alternate Billing Services/Line Information Data Base (ABS/LIDB), CLASS Calling Name Delivery (CNAM), Message Waiting Service (MWS), 891 Calling Card Service, Private Virtual Network Service (PVN), 800 Database Service, IS-41 Message Transport Service, and AIN Services.

The information provided in Appendix H is intended to serve as guidelines for STP suppliers, indicating potential services to be supported by the GTT function at STPs. For these guidelines to be useful, STP suppliers must determine which of the services will be provided by the Bccs.

H.2 General Assumptions

Worst case estimates have been derived for the services discussed in the next sections, based on the assumption that STPs are able to support 10-digit GTT as well as range entries, although most of the services only require 6-digit GTT. With respect to memory requirements, it is assumed that an entry encompassing a range of global titles is equivalent to a non-range entry. Therefore, both range and non-range entries will be counted as one entry.

It is assumed that the data items administered as a global title entry include the following: a Global Title (GT), a Routing Indicator (RI), up to four Destination Point Codes (DPCs) designating destinations with replicated applications, as well as up to four Subsystem Numbers (SSNs) and associated costs. It should be noted that not all services require GTT table entries with multiple destinations with their associated SSNs and costs. Backup destinations are included where applicable.

Worst case estimates for some services may depend on the method used for routing interLATA/internetwork queries or queries associated with interLATA calls. For example, after a GTT is performed to determine a DPC, LIDB queries are either MTP routed within a network, or if destined to another network, MTP routed through a Hub provider (i.e., the resulting DPC is in the destination network, not in an Interconnecting CCS Network, e.g., Hub, Interexchange Carrier). InterLATA or internetwork CLASS messages, however, may be addressed to an ICN for routing. If a method has not yet been chosen for a particular service, the effects of both routing options on GTT table sizes are considered. It should be
noted that here, MTP routing refers to messages being MTP routed from the STP performing the GTT. It should not be assumed that the messages are MTP routed directly from the originating Common Channel Signaling Switching Office (CCSSO).

H.3  Worst-Case Estimates

In Table H-1, the entry “11,000 - 8 NPAs/LATA” implies that assuming there are 8 NPAs per LATA, the number of entries required is up to 11,000.

Table H-1.  Worst Case Estimates

<table>
<thead>
<tr>
<th>Service</th>
<th>Routing Method</th>
<th>Worst Case Number of Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MTP thru Hub</td>
<td>Handoff to ICN</td>
</tr>
<tr>
<td>CLASS AC/</td>
<td>x</td>
<td>11,000 8 NPAs/LATA&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>AR/SLE</td>
<td></td>
<td>10,000 8 NPAs/LATA</td>
</tr>
<tr>
<td>CLASS CNAM</td>
<td>x</td>
<td>22,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12,000</td>
</tr>
<tr>
<td>ABS/LIDB</td>
<td>x</td>
<td>27,000</td>
</tr>
<tr>
<td>891 Service</td>
<td></td>
<td>1,000</td>
</tr>
<tr>
<td>PVN</td>
<td></td>
<td>3,200 8 NPAs/LATA</td>
</tr>
<tr>
<td>MWS</td>
<td>x</td>
<td>11,000 8 NPAs/LATA&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10,000 8 NPAs/LATA</td>
</tr>
<tr>
<td>800 Service</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>IS-41 Message Transport</td>
<td></td>
<td>8,700&lt;sup&gt;b&lt;/sup&gt;</td>
</tr>
<tr>
<td>Inter-network AIN (TT=8)</td>
<td></td>
<td>260&lt;sup&gt;c&lt;/sup&gt;</td>
</tr>
<tr>
<td>PCS (AIN)</td>
<td></td>
<td>8&lt;sup&gt;d,e&lt;/sup&gt;</td>
</tr>
<tr>
<td>Area Wide Centrex (AIN)</td>
<td></td>
<td>46&lt;sup&gt;c&lt;/sup&gt;</td>
</tr>
<tr>
<td>Switch Redirect</td>
<td></td>
<td>46&lt;sup&gt;c&lt;/sup&gt;</td>
</tr>
<tr>
<td>Outgoing Call Restriction (AIN)</td>
<td></td>
<td>46&lt;sup&gt;c&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

Notes to Table H-1.

a. These estimates are based on the assumption that signaling for non-Bcc switching offices (i.e., those owned by independent telephone companies) is provided by the Bcc serving the independent’s area. If all independents provide their own signaling, or contract with other network providers for signaling, this estimate could increase by 12,000 entries.

b. This estimate includes the number of GTT entries necessary to support the transport of IS-41 messages destined to a Home Location Register for both PCS and non-PCS.
wireless. The PCS-specific portion of this estimate, which is 3200 entries, is based on the assumptions that 6-digit GTT can be used, and that up to 4 dedicated NPAs will be used for PCS (prior to PCS number evolution to service provider portability). Note that GTT on at least 8 digits of the global title address will be required in some cases for non-PCS wireless.

c. The estimate for TT 8, which is defined for inter-network AIN messages, requires the use of 10-digit GTT. The estimate provided is based on two assumptions. There are approximately 220 STP pairs that could perform a final GTT. In addition, once at the STP performing the final GTT, up to 40 destinations/subsystem number pairs may be supported.

d. The estimate for the AIN portion of PCS is based on the assumption that 6-digit GTT can be used, and that up to four dedicated NPAs will be used prior to PCS number evolution to PCS service provider portability. It is assumed that two 6-digit range entries per NPA is sufficient to route to the desired destination. If a particular Bcc needs the flexibility to select the destination for each NPA-NXX individually, then up to 3200 entries [i.e., (4 NPAs)*(800 possible NXXs)] could be needed.

e. These AIN services may use the same TT, or different TTs, depending on network-specific characteristics such as the release of AIN, and the use of subsystem numbers. If different translation types are used, some of the data could potentially be shared using the multi-step GTT capability. The estimates were derived on the assumptions that a Bcc STP could be responsible for performing GTT for global title addresses consisting of, at most, 23 NPAs. In addition, it is assumed that the use of two 6-digit range entries per NPA is sufficient to route to the desired destination. If a particular Bcc needs the flexibility to select the destination for each NPA-NXX individually, then up to 18,400 entries [i.e., (23NPAs)*(800 possible NXXs)] could be needed. In addition, the GTT table impacts of only a subset of potential AIN services described here. Bccs may be offering additional AIN services, or a completely different subset of AIN services.

H.4 Refining Worst-Case Estimates

The worst case estimates provided may be unrealistically high for some services, while acceptable approximations for others. To obtain more accurate estimates, if necessary, network-specific characteristics need to be examined. Many of the worst case estimates provided are based on the assumption that range entries cannot be used in some situations, more specifically that no contiguous global titles map to the same PC. For example, the worst case estimate for CLASS features (AC, AR, SLE) is based on the assumption that, within a LATA, no contiguous NPA-NXXs are assigned to a particular Ccsso. This implies that 800 entries may be needed for an NPA within a particular LATA. To obtain a more accurate estimate of the number of entries, the number of contiguous NPA-NXXs per Ccsso within a particular LATA must be determined. Similar assumptions were used for
the other services, where the use of range entries may significantly reduce the worst case estimates. Since the use of range entries depends on network specific characteristics, each network must be assessed independently. In addition, some of the estimates were derived using current network information. As such, the use of additional NPA-NXXs may affect the estimates provided.

H.5 Related Issues

This section provides additional information pertaining to the memory requirements for GTT tables at STPs. An area that will affect the memory requirements for GTT tables at STPs is the consolidation of GTT information. Many tables may include identical global title to PC information, wasting memory capacity by storing redundant information. For example, a final GTT on an NPA-NXX for a CLASS feature will result in the PC of the CCSSO serving that NPA-NXX. For MWS, a final GTT on the same NPA-NXX will also result in the PC of the CCSSO serving that NPA-NXX. This global title to PC information may potentially be stored several times, once for each service or set of services that uses the same global title to PC data.

To reduce the memory capacity STPs require for GTT tables, multi-step GTT requirements have been provided to consolidate some of the data, thus avoiding the storage of redundant information. These requirements will allow some of the otherwise redundant GTT tables to be shared by several translation types.
Appendix I: Estimates of Global Title Translation Capacity

I.1 Introduction

Increasing demand for transaction-based services such as Advanced Intelligent Network (AIN) services, 800 service, Personal Communication Services (PCS) etc., results in an increasing penetration of TCAP messages into the CCS network. This increase in penetration level has potential impacts on the performance of STPs due to the processing required by these messages. Many of the transaction-based services require interactions between service providing applications and databases located at the SCPs and the SSPs invoking the services. The results of such interactions are conveyed over the CCS network as query, response, or conversation type TCAP messages. The query messages need to have Global Title Translation (GTT) at the STPs to reach the service-providing platform at the SCP. The increasing number of GTTs per STP due to increasing service penetration results in greater utilization of the STPs’ translation performing resources.

The purpose Appendix I is to estimate the load offered to STPs for GTT due to the increasing number of TCAP messages. The estimates presented in this appendix are expected to provide guidelines to Bccs and suppliers about how large the need of increasing service penetrations may be on STPs’ translation resources. The results in Section I.4 provide worse case estimates obtained for the engineered failure mode link load of 0.8 erlang and are dependent on the service penetration levels and the service-related messages considered in the estimation process.

The estimates are given in terms of the number of translations done on a per link basis to directly provide results for distributed STP implementations where link processors perform GTT. These results can be used to estimate the GTT load for an STP implementation with a centralized processing unit performing GTT, as discussed further in Section I.4.

The information presented in the tables in Section I.4 are for planning purposes only since the signaling network deployment and the demand for a particular service vary between network providers. Different network architectures and service deployment strategies considered in this appendix do not represent all possible configurations and alternatives. Consequently, estimates given in Section I.4 may not be valid for other network topologies and service deployment plans. The estimates will be revised in the future if more details can be obtained about the network-specific input such as network topology, service deployment strategy for various types of services, services mix, and service related parameters.

I.2 Services and Service-Related Assumptions

This section lists the services considered in the estimation study and explains the assumptions related to the number of messages and the length of messages corresponding to each service. In the following sections, local and regional STP pairs are denoted by LSTP
and RSTP, respectively. The traffic carrying messages that may result in GTT at a LSTP pair is the traffic destined to the pair from its local SSPs. The traffic carrying messages that may result in GTT at a RSTP pair is the traffic destined to the pair from LSTPs attached to it or in certain cases (depending on the network architecture) the traffic destined to the pair from its local SSPs. Each of these traffic streams is hereinafter referred to as *upstream traffic* and has been of interest in the GTT capacity estimation study. Hence, only the messages that may be observed in the upstream traffic are considered below.

- **POTS (interoffice):** POTS service is treated as equivalent to call setup signaling. Each SS7 call originated in the network needs call setup signaling regardless of any additional services (such as 800, CLASS feature, etc.) requested by the user originating the call. If the user does not request any additional service, the call is identified as a POTS call. During a call setup, three, four, five, six, or seven of the following ISDNUP messages are assumed to be sent between two switches. (SUS message is sent if the called party releases the call; ANM message is sent if the called party answers the call; COT is assumed to be sent for one in eight calls originated.)

  The messages and their approximate lengths are listed below.

  - IAM = 48 octets
  - ACM = 20 octets
  - REL = 22 octets
  - RLC = 17 octets
  - ANM = 18 octets
  - SUS = 19 octets
  - COT = 18 octets.

  All seven of these messages exist in the upstream traffic because there are calls generated and received in both directions. For example, the traffic on an A-link from a SSP to a LSTP have all seven message types present assuming there are both outgoing calls from the SSP and incoming calls to the SSP. However, some of these messages may appear more frequently than others depending on the ratio of the number of calls originated at a SSP to the calls terminated at the same SSP. It is assumed that the *interoffice* call volume generated by each SSP is approximately the same and is equally distributed among other SSPs. Therefore, when the traffic to an LSTP pair from its local SSPs (or the traffic to an RSTP pair from its LSTPs, if all the local and regional STP pairs are in the same LATA and D-links are used to carry call setup signaling) is observed for a long time, IAM, REL and RLC messages appear in the traffic with approximately equal probability. An ACM message is assumed to be sent for 90% of the calls originated (an ACM message is not sent if the called party's line is busy and release on busy is done). An ANM message is assumed to be sent for 80% of the calls originated. A COT message is assumed to be sent for one in eight calls originated. A SUS message is sent only if the called party releases the call and the
number of calls released by the called party is assumed to account for 25% of all of the calls completed.

- **CLASS Feature:** Automatic CallBack (AC) and Automatic Recall (AR) services are considered in the estimation study. It is assumed that the following five messages are sent for an AC or AR activation:
  - Initial Query = 121 octets
  - Initial Response = 66 octets
  - Terminating Scanning Query = 80 octets
  - Terminating Scanning Conversation = 51 octets
  - Terminating Scanning Response = 50 octets.

All five of these messages are assumed to exist in the upstream traffic for intraLATA activations. (InterLATA CLASS activations are not considered because the interLATA TCAP message routing issue has not been resolved yet and the market penetration of interLATA CLASS services is unknown. However, for certain interLATA TCAP routing options, the interLATA queries will result in GTT at an STP in the destination LATA and hence these messages will increase the translation load offered to the STP. However, for small market penetration of interLATA CLASS services, this increase in the translation load is not expected to be significant.) It is assumed that all five of these CLASS messages appear in the upstream traffic with approximately equal probability. Of these five messages, only the Initial Query message is routed on global title and thus requires GTT at STP.

- **800:** One query and one response message are assumed to be sent for an 800 call. It is assumed that only the query message is present in the upstream traffic.
  - Query = 90 octets.

- **ABS:** One query and one response message are sent for an ABS call. For the same reason as in the case of 800 service, only the query message is considered.
  - Query = 94 octets.

- **PCS:** Two messages are assumed to be present in the upstream traffic.
  - Info_Analyze = 106 octets
  - RegistrationNotification = 82 octets.

  Info_Analyze is an AIN query message sent from the AIN SSP to an AIN SCP. RegistrationNotification is an IS-41 query message sent to register a roaming hand set with the PCS Service Provider. It is assumed that 10% of the PCS calls require registration of the roamers.

- **Calling Name Delivery (CNAM):** Only one query message is present in the traffic destined to the STPs for translation.
• **AIN**: It is assumed that four messages are needed per call requesting an AIN service. Two of these four messages are sent by the SSP communicating with the service logic at an AIN SCP. One of these two messages is a query message and the other one is a conversation message. Only the query needs GTT performed at an STP. The conversation message uses the SCCP Calling Party Address field of the corresponding response and hence is transported back to the SCP via MTP routing. It is assumed that the length of each of these two messages is 150 octets.

— Query= 150 octets

— Conversation= 150 octets.

• **Signaling Interconnection Service (SIS)**: SIS is a tariffed interconnection service in which a SIS Provider’s STPs provide intraLATA routing of ISUP and TCAP messages between Interconnecting CCS Networks (ICNs). Potential subscribers to SIS include small Interexchange Carriers (IXCs), Independent Local Exchange Carriers (ILECs), Competitive Local Exchange Carriers (CLECS), and Alternate Access Providers (AAPs).

SIS would offer transport of ISUP messages for call setup, and transport of TCAP messages (e.g., ABS, CLASS, 800 Service) for database lookups to potential subscribers. SIS could be offered to a small LEC, for example, who does not have an STP pair in their network and requires a second party (i.e., Bcc) to provide them with interconnection to other CCS networks. Three types of routing may be provided in support of SIS: MTP routing, OPC-DPC routing, and SCCP\(^1\) routing (i.e., routing requiring GTT). If the SIS provider performs SCCP routing, then the GTT capacities will be affected. The impacts to capacities will depend on the services provided by the SIS subscriber to their customers. The number and length of messages related to each service provided by SIS will be the same as those mentioned previously in this subsection.

Table I-1 summarizes the relative service penetration level of the signaling services and the number of associated messages that need GTT.

---

1. OPC-DPC routing is a new routing method currently proposed and described in Issue 13-114 in GR-82-ILR, Issue 1C, December 1995.
I.3 Network Architectures

The different network models considered in STPs’ GTT capacity estimation are described in this section. These models have been primarily differentiated by alternative deployment strategies for service logic as well as by the grouping of LSTP pair(s) and an RSTP pair in the same LATA.

I.3.1 Network Model 1

In the first network model, illustrated in Figure I-1, the SCPs are deployed at both the local and the regional level. Each LSTP and RSTP pair hosts one pair of SCPs referred to as the LSCP and RSCP pair, respectively. All three STP pairs serve as “local” transfer points to a cluster of adjacent SSPs. Four subcases are described below.
I.3.1.1 Model 1.a

The LSCP pairs host AIN, PCS, and CNAM service information. The RSCP pair hosts 800 and ABS applications and databases on a regional basis as well as AIN, PCS, CNAM service information for the SSPs adjacent to the RSTP pair. Each STP pair (local or regional) performs GTT for query messages sent by their adjacent SSPs for AIN, PCS, and CNAM services. The RSTP pair also performs GTT for query messages from all the SSPs for 800 and ABS services. For this subcase, it is assumed the RSTP pair and at least one LSTP pair are in the same LATA. Therefore, call setup and CLASS messages appear on A-links as well as on D-links (because the SSPs subtended at the RSTP and at the LSTP pairs are in the same LATA and therefore D-links can be used to carry CLASS and call setup messages).

I.3.1.2 Model 1.b

In terms of service deployment at local and regional levels, this model is identical to model 1.a. The only difference is that here it is assumed that RSTP and LSTP pairs are all in different LATAs, and thus there is not any call setup and CLASS related signaling traffic on the D-links (call setup signaling is directed to an IC network).

I.3.1.3 Model 1.c

This model is similar to model 1.a. The only difference is that the CNAM service information is centralized at the regional level. That is, no LSCP has the CNAM service information. All the queries destined to CNAM service logic at the RSCP are translated by the RSTP pair.
I.3.1.4 Model 1.d

This model is similar to model 1.b. The only difference is that the CNAM service information is centralized at the regional SCP pair. That is, no LSCP has the CNAM service information. All the queries destined to CNAM service logic at the RSCP are translated by the RSTP pair.

I.3.2 Network Model 2

The second network model, illustrated in Figure I-2, represents the case where the LSTPs are in the same LATA and are connected via B-links. For this configuration, the location of the RSTP pair (whether it is in the same LATA with the LSTP pairs or not) does not change the traffic mix on the A- and D-links, and call setup signaling traffic is assumed to be absent on the D-links. If the RSTP pair is in a different LATA, call setup signaling is directed to an IC network. If the RSTP pair is in the same LATA with the LSTP pairs, then the assumption of not having call setup signaling on the D-links is still valid if the B-links are part of the normal routes for signaling between SSPs subtended at different LSTP pairs and if routing can be done on the normal routes. Four subcases are considered below.

![Network Model 2 Diagram]

**Figure I-2.** Network Model 2

I.3.2.1 Model 2.a

AIN, PCS, and CNAM service logics are located at each LSCP pair. The RSCP pair hosts 800 and ABS applications and databases on a regional basis. The RSTPs perform GTT for queries destined to 800 and ABS applications. Translations for AIN, PCS, CNAM, and CLASS feature queries sent by SSPs that are adjacent to an LSTP are done by that LSTP. Model 2.a assumes that one LSCP pair at each LSTP pair exists.
I.3.2.2 Model 2.b

Only one LSCP pair (hosting the AIN platform, PCS, and CNAM service information) exists at the local level. Each LSTP pair performs GTT on queries sent by its adjacent SSPs and routes them to the LSCP. An example of this architecture is where only the right LSCP pair exists and is connected to the right LSTP pair (see Figure I-2). Both the left and the right LSTP pairs perform GTT for TCAP queries destined to the LSCP.

I.3.2.3 Model 2.c

This model is similar to model 2.a. The only difference is that the CNAM service information is centralized at the regional level. That is, no LSCP has the CNAM service information. All the queries destined to CNAM service resources at the RSCP are translated by the RSTP pair.

I.3.2.4 Model 2.d

This model is similar to model 2.b. The only difference is that the CNAM service information is centralized at the regional level. That is, no LSCP has the CNAM service information. All the queries destined to CNAM service resources at the RSCP are then translated by the RSTP pair.

I.3.3 Network Model 3

The third network model, illustrated in Figure I-3, represents a centralized architecture where all of the services are located at the RSCP pair. Three subcases are considered for this model. For all of three subcases, translations for messages associated with 800, ABS, AIN, PCS, and CNAM services are performed at the RSTP pair.

![Figure I-3. Network Model 3](image-url)
I.3.3.1 Model 3.a

The RSTP pair and at least one LSTP pair are in the same LATA. Therefore, call setup signaling related to calls destined to SSPs subtended from different STP pair(s) in the LATA exists on D-links.

I.3.3.2 Model 3.b

All of the STP pairs are assumed to be located in different LATAs. Call setup signaling for calls destined to SSPs homed at different STPs is handed over to an IC network and, therefore, no call setup signaling exists on the D-links.

I.3.3.3 Model 3.c

There are no SSPs subtending from the RSTP pair. The RSTP pair is in charge of performing GTT and routing of TCAP messages destined to the RSCP pair. The RSCP pair hosts 800, ABS, AIN, PCS, and CNAM service information. The RSTP pair and an LSTP pair may or may not be in the same LATA; this does not change the upstream traffic.

I.3.4 Network Model 4

The fourth model, illustrated in Figure I-4, is a centralized architecture for which the LSTP pairs are located in the same LATA and are interconnected via B-links. As discussed for the network model 2, the location of the RSTP pair with respect to the LSTP pairs does not have an impact on the GTT estimation results. Using a similar argument to the one given for the network model 2, it is assumed the D-links do not carry any call setup signaling.

![Network Model 4 Diagram]

Figure I-4. Network Model 4
I.4 Service Impacts on GTT Information

I.4.1 Traffic Mix and GTT Information

This section provides information about the presence of service messages on A- and D-links, and whether GTT associated with these messages is performed at the local or regional STP level, for each network model described in Sections I.3.1, I.3.2, I.3.3, and I.3.4. Tables I-2 and I-3 present this information.

In these tables, a dash (-) indicates that the messages related to a particular service do not appear in the traffic observed on the corresponding links. The letters Y and N indicate the presence of messages related to a service on corresponding links, and Y indicates that GTT for the messages is performed at the STP pair connected to the links (i.e., A-links for Table I-2 and D-links for Table I-3). For example, for network model 1.a, AIN messages are absent on the D-links to the RSTPs and therefore a dash is indicated in the box corresponding to AIN services and the model 1.a. On the other hand, messages associated with 800 service are present on both A-links from SSPs to STPs and D-links. However, GTT for 800 query messages are performed at the RSTP level (indicated by Y in the corresponding box in Table I-3) but not at the LSTP level (indicated by N in the corresponding box in Table I-2).

Table I-2. Traffic Mix for Messages Received at STPs on A-links from Adjacent SSPs

<table>
<thead>
<tr>
<th>Network Models</th>
<th>Call Setup</th>
<th>800</th>
<th>ABS</th>
<th>AIN</th>
<th>PCS</th>
<th>CLASS</th>
<th>CNAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.a, 1.b, 2.a, 2.b</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>1.c, 1.d, 2.c, 2.d</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>3.a, 3.b, 3.c, 4</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>

Table I-3. Traffic Mix for Messages Received at RSTP pair on D-links from LSTP Pairs

<table>
<thead>
<tr>
<th>Network Models</th>
<th>Call Setup</th>
<th>800</th>
<th>ABS</th>
<th>AIN</th>
<th>PCS</th>
<th>CLASS</th>
<th>CNAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.a</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>-</td>
<td>-</td>
<td>Y</td>
<td>-</td>
</tr>
<tr>
<td>1.c</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>-</td>
<td>-</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>1.b, 2.a, 2.b</td>
<td>-</td>
<td>Y</td>
<td>Y</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1.d, 2.c, 2.d</td>
<td>-</td>
<td>Y</td>
<td>Y</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Y</td>
</tr>
<tr>
<td>3.a</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>3.b, 3.c, 4</td>
<td>-</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>-</td>
<td>Y</td>
</tr>
</tbody>
</table>
The traffic mix and the GTT estimation for B-links are not given in these tables. It is assumed that for messages carried over B-links, GTT, if necessary, is performed at the STP pair which is adjacent to SSPs originating the messages. That is, if at most one GTT per given message is assumed to be performed, then it can be inferred that any message on B-links is MTP routed to its final destination and thus no results are provided for messages received on B-links.

I.4.2 SIS Impacts on GTT Capacity

A SIS subscriber that offers TCAP-based services to its customers requires the SIS provider’s network to support SCCP routing to the destinations specified by the SIS subscriber. The impact on GTT capacity will be a function of the TCAP-based services (e.g., ABS, CLASS, 800 Service) offered by the SIS subscribers to their customers and the number of SIS subscribers requiring GTTs by the SIS provider. Given this information, the impact on the GTT capacity is determined from the service information in Section I.2, Table I-2, and Table I-3.

I.5 Results

This section presents estimates of the number of GTTs/link/sec for different network models and different service penetration levels. Table I-4 summarizes the number of GTTs/A-link/sec at the STP pair (LSTP pair or, for network models 1.a, 1.c and 3.a, RSTP pair as well) adjacent to the SSPs sending the messages, for different service penetration levels. Table I-5 summarizes the number of GTTs/D-link/sec at the RSTP pair for different service penetration levels. In both tables, only the varied penetration levels are shown. (Recall that the other services penetrations are either fixed to a certain percentage or to a fixed percentage of the relative penetration of another service, as Table I-1 shows.)

Table I-4. Number of Translations at a STP Adjacent to SSPs Sending TCAP Messages

<table>
<thead>
<tr>
<th>% Service Penetration</th>
<th>GTT/A-link/sec for Network Models</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>800</td>
</tr>
<tr>
<td>5.0</td>
<td>2.5</td>
</tr>
<tr>
<td>5.0</td>
<td>5.0</td>
</tr>
<tr>
<td>5.0</td>
<td>2.5</td>
</tr>
<tr>
<td>10.0</td>
<td>2.5</td>
</tr>
<tr>
<td>10.0</td>
<td>5.0</td>
</tr>
<tr>
<td>10.0</td>
<td>2.5</td>
</tr>
<tr>
<td>10.0</td>
<td>5.0</td>
</tr>
<tr>
<td>10.0</td>
<td>10.0</td>
</tr>
</tbody>
</table>
Table I-5. Number of Translations at a RSTP Connected to LSTP Pair(s)

<table>
<thead>
<tr>
<th>% Service Penetration</th>
<th>800</th>
<th>PCS</th>
<th>AIN</th>
<th>POTS</th>
<th>GTT/D-link/sec for Network Models</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5.0</td>
<td>2.5</td>
<td>2.5</td>
<td>84.5</td>
<td>1.a, 1.c, 1.b, 2.a, 2.b, 1.d, 2.c, 2.d, 3.a, 3.b, 3.c, 4</td>
</tr>
<tr>
<td></td>
<td>5.0</td>
<td>5.0</td>
<td>2.5</td>
<td>82.5</td>
<td>10.4, 10.9, 62.0, 62.7, 14.8, 49.5</td>
</tr>
<tr>
<td></td>
<td>5.0</td>
<td>2.5</td>
<td>5.0</td>
<td>82.5</td>
<td>10.4, 12.2, 62.0, 63.3, 16.0, 43.8</td>
</tr>
<tr>
<td></td>
<td>10.0</td>
<td>2.5</td>
<td>2.5</td>
<td>79.0</td>
<td>18.0, 18.8, 62.0, 62.3, 20.2, 52.3</td>
</tr>
<tr>
<td></td>
<td>10.0</td>
<td>5.0</td>
<td>2.5</td>
<td>76.5</td>
<td>18.0, 18.8, 62.0, 62.3, 22.8, 53.4</td>
</tr>
<tr>
<td></td>
<td>10.0</td>
<td>2.5</td>
<td>5.0</td>
<td>76.5</td>
<td>18.0, 19.4, 62.0, 62.7, 21.4, 47.7</td>
</tr>
<tr>
<td></td>
<td>10.0</td>
<td>5.0</td>
<td>5.0</td>
<td>74.0</td>
<td>17.6, 19.0, 62.0, 62.7, 22.5, 48.6</td>
</tr>
<tr>
<td></td>
<td>10.0</td>
<td>10.0</td>
<td>10.0</td>
<td>64.0</td>
<td>17.6, 20.2, 62.0, 63.4, 25.6, 45.2</td>
</tr>
</tbody>
</table>

For network models 1.b, 2.a, 2.b, the number of translations per D-link at an RSTP is 62.0 and is based on failure mode traffic load of 0.8 erlang on a D-link. This result is insensitive to the changes in penetration levels because only 800 and ABS related messages are assumed to appear on the D-links and the only variable is the penetration of 800 service (recall that ABS penetration level is 10% of that of 800).

The results are given in terms of the number of translations done on a per-link basis to directly provide results for distributed STP implementations where link processors perform GTT. For an STP implementation with a centralized processing unit performing GTT, the results presented in Table I-4 can be multiplied by the number of links from SSPs incoming to the LSTP (or to the RSTP for network models 1.a and 3.a) to estimate the translation load offered to the processing unit. For an RSTP with a centralized processor unit, the D-link estimation results from Table I-5 should be multiplied by the appropriate number of D-links (assuming that all of the D-links carry the same traffic mix) and the A-link estimation results from Table I-4 should be multiplied by the number of A-links for any SSPs adjacent to the RSTP. The two numbers should then be added to obtain the total offered translation load to the RSTP. These results for an STP with a centralized processing unit are thus based on the assumption that 0.8 erlang traffic exists on all the links used in the computation.

To calculate the average translation load offered to an STP under normal link utilization conditions (i.e., links carrying 0.4 erlang traffic), the results Tables I-4 and I-5 present can be divided by two. Thus, the aggregate offered translation load to an STP can then be easily calculated for cases where links carry different amounts of traffic (i.e., the link utilization level is not uniform across all the links considered in the network).

Despite the increase in the load offered to the STP’s processing units, the STP should be able to meet the criteria (i.e., the STP node processing time for normal and failure mode loading) given in Section 8.2.1 of this GR. This information is, for the reader’s convenience, replicated in Table I-6.
Table I-6. STP Node Processing Time

<table>
<thead>
<tr>
<th>Loading</th>
<th>STP Node Processing Time (ms)</th>
<th>Mean</th>
<th>95%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td></td>
<td>43</td>
<td>&lt;= 79</td>
</tr>
<tr>
<td>Failure</td>
<td></td>
<td>80</td>
<td>&lt;= 202</td>
</tr>
</tbody>
</table>
Appendix J: Operations Requirements to Support SCCP Functions

Appendix J provides detailed operations requirements for the following SCCP functions:

- Multi-Step Global Title Translation (Section J.1)
- UDT/XUDT Message Processing (Section J.2).

The operations requirements provided in this appendix consists of provisioning and surveillance requirements. The provisioning requirements are described in terms of the Provisioning Data Elements, the Data Operations, and the Database Management Functions.

As part of the provisioning data element description, the following notation is used:

- alphabetic(x) - meaning an ASCII alphabetic character string of up to x characters.
- alphanumeric(x) - meaning an ASCII alphanumeric character string of up to x characters.
- alphanumeric/graphic(x) - meaning an ASCII character string containing up to x alphanumeric and graphic characters.
- numeric(x) - meaning an ASCII numeric character string of up to x characters. [All numeric character strings are base-10 (decimal) format.]

Some data elements are of fixed length, meaning they must always have the maximum length specified. Others may be of variable length having from one character up to and including the maximum number of characters.

Data operations refer to the commands or transactions to be applied to the provisioning data elements. As such, the STP is required to process commands that may be used to add, update, change, or delete the provisioning data described in this appendix. These are referred to as Recent Change (RC) commands. The STP is also required to process commands that are used to review the provisioning data. These are referred to as Verify (V) commands.

The database management functions refer to the database administration functions required for the data.

In general, surveillance activities are designed to assist in the identification of abnormal conditions and failures in the network, and to assist in isolating troubles to a specific node or component of the network. As such, surveillance requirements consist of event notification and measurement requirements. The event notification requirements identify the events that should be reported by an STP to CCS network personnel, as well as the format and contents of the notification. The surveillance measurement requirements aid in troubleshooting the specific cause when an event occurs.
J.1 Operations Requirements for the Multi-Step GTT Function

This section provides the operations requirements that are needed to provide the ability to perform the Global Title Translation (GTT) function in several steps.

J.1.1 Overview

To reduce the demand on memory at the STPs, it is required that the GTT function be able to be performed in several steps for any given Translation Type (TT). One step in the GTT function would map a TT to a specific Subsystem Number (SSN) (i.e., TT-to-SSN mapping). Another step would determine a Destination Point Code (DPC) based on the Global Title Address (GTA) that is provisioned. More specifically, a GTA would be mapped to a specific DPC (i.e., GTA-to-DPC mapping) or mapped to a set of ordered DPC data (i.e., GTA-to-Ordered DPC mapping), where a specific DPC is determined from the set of ordered DPC data based on a relative cost value.

Performing the GTT function in several steps allows for the consolidation of portions of GTT data when there is significant overlap for different applications (i.e., redundant GTT data). Not only will the demand on STP memory be reduced, but considerable work effort in provisioning GTT data can be saved by consolidating identical portions of the data. It is important to note the existing GTT data structure may be used, if desired, for any given TT, as Section 4.3.1.1 describes.

To support the consolidation of GTT data stored at STPs, the following three categories of provisioning data are defined:

A. Multi-Step GTT: TT-to-SSN Mapping Translation

B. Multi-Step GTT: GTA-to-DPC Mapping Translation

C. Multi-Step GTT: Ordered DPC Translation

TT-to-SSN Mapping Translation data is used to map a Translation Type (TT) to a specific Subsystem Number (SSN). Each unique TT/SSN data combination will be associated with a GTA Reference which will be used to “point to” or “reference” a specific set of GTT data within the GTA-to-DPC Mapping Translation data that should be used to assist in the translation of the GTA of the SS7 message to a DPC. By reusing the GTA Reference across TTs, the same GTA-to-DPC translations may be used for multiple applications or services. This is the likely mode of use for switched-based services where NPA-NXX GTAs shall be mapped to CCS switching office/SSP DPCs. The GTA Reference may also be used to reference GTT data currently supported by the existing STP data structure to temporarily ease the transition to the proposed new GTT data structure or to permanently retain the existing GTT data structure, depending on whether or not an STP supplier will support the new GTT data structure. To reference the existing ordered GTT data structure, the TT should be mapped to a null SSN and null GTA Reference. As such, the TT value would be
used to reference the set of existing GTT data that should be used to perform the GTT function.

The purpose of GTA-to-DPC Mapping Translation data is twofold: 1) to map one or more GTAs to a specific DPC or capability code (i.e., GTA-to-DPC mapping), or 2) to map one or more GTAs to an Ordered GTA Reference that will be used to “point to” or “reference” a specific set of ordered DPC data within the Ordered DPC Translation data (i.e., GTA-to-Ordered DPC Reference mapping). As such, the GTA(s) defined by GTA-to-DPC Mapping Translation data will be associated with either a DPC and routing indicator (to indicate whether or not a subsequent GTT should be performed for the message), or an Ordered DPC Reference. In general, any message requiring a subsequent GTT (i.e., the DPC is the capability code of another mated STP pair) or for which the GTT results in a DPC that is not a replicated application (i.e., switch-based service) will use a GTA-to-DPC/RI mapping scheme. Any message for which the GTT Multi-Step GTT: Ordered DPC Translation results in a DPC of a replicated application (i.e., database application) will use a GTA-to-Ordered DPC Reference mapping scheme.

Ordered DPC Translation data is used to define one or more DPCs that should be used to determine where an SS7 message should be sent. An Ordered DPC Reference will be used to uniquely identify a specific set of DPC data that should be used to perform the GTT function. The GTT function will determine a specific DPC within the set of ordered DPC data based on a relative cost value that is used to indicate the routing preference for the SS7 message.

Since SSN values are not standardized, an SSN used to represent a given application in one network may not be the same SSN value to represent the same application in another network. As a per-Bcc option, an “override” SSN value may need to be provisioned for the DPC defined in the GTA-to-DPC Mapping Translation data or Ordered DPC Translation data. The “override” SSN value, if specified, will be used to override the SSN value specified in the TT-to-SSN Mapping Translation data. It is important to note that SCCP Application data, described in Section J.2, is required to support the multi-step GTT process in order to verify that the DPC and SSN that result from a GTT, and to which a message will be routed, is valid (i.e., verify the application at the node is supported).

### J.1.2 Provisioning Requirements

#### J.1.2.1 Provisioning Data Elements

This section provides a detailed description of the provisioning data that is required to support GTT data.
A. Multi-Step GTT: TT-to-SSN Mapping Translation

**RJ-1** [527] The STP shall permit the provisioning of TT-to-SSN Mapping Translation data to map a TT to a specific SSN.

**RJ-2** [528] The STP shall permit the provisioning of the following data item for TT-to-SSN Mapping Translation data:

- *Translation Type (TT)* - numeric(3), fixed length; the identification of the type of allowed GTT corresponding to a particular application or set of applications. This attribute is the decimal representation of the 1-octet binary value contained in the TT field of the SCCP Called Party Address (CdPA) of the SS7 message being translated. Valid TTs are 001 through 254.

**RJ-3** [529] The STP shall permit the provisioning of the following data items for each TT uniquely provisioned:

- *Subsystem Number (SSN)* - numeric(3), fixed length; the identification of the application software subsystem at the destination node that should receive and process the message. This attribute is comprised of the decimal representation of the 1-octet binary value to be placed in the translated message's CdPA SSN. Valid SSNs are: 1) null, 2) 000, and 3) the range of 002 through 255 (NOTE: The value 001 is reserved for SCCP management messages and are not valid for GTTs). A null SSN indicates the existing GTT data structure will be used to perform the GTT for the SS7 message for the given TT. The value 000 denotes that the STP shall populate the CdPA SSN with zeroes, representing an “unknown” SSN. Values between 002 and 255 convey specific application subsystems at signaling end points.

- *GTA Reference* - alphanumeric(8), variable length; identifies a set of translation data within the GTA-to-DPC Mapping Translation data that should be used by the translation method in the GTT process. A null GTA Reference indicates the existing GTT data structure will be used to perform the GTT for the SS7 message (i.e., the GTT process will use the existing ordered GTT data provisioned at STPs).

**OJ-4** [530] It is desirable that the STP permit the provisioning of the following data item for each TT/SSN/GTA Reference data combination:

- *Remarks* - alphanumeric(20), variable length; a user-specified comment field that may be used to provide a brief description of the objective/purpose of the GTT to be performed.

---

1. Note that a null SSN does not represent the non-null value of 000.
B. Multi-Step GTT: GTA-to-DPC Mapping Translation

RJ-5  [531] The STP shall permit the provisioning of GTA-to-DPC Mapping Translation data to map one or more GTAs to a DPC (or capability code) and routing indicator when the DPC of the SS7 message should be an STP (or mated STP pair) that will perform a subsequent GTT for the SS7 message or the DPC of the SS7 message should be a non-replicated application (e.g., CCS switching office).

RJ-6  [532] The STP shall permit the provisioning of GTA-to-DPC Mapping Translation data to map one or more GTAs to an Ordered DPC Reference when the GTA should be mapped to a set of ordered DPCs as defined by the Ordered DPC Translation data.

RJ-7  [533] The STP shall permit the provisioning of the following data items for GTA-to-DPC Mapping Translation data:

...  GTA Reference - alphanumeric(8), variable length; identifies one or more GTAs that should be used in the GTT process.

...  Global Title Address (GTA) - alphanumeric(10), variable length; the non-SS7 address that requires translation to a DPC or DPC-SSN SS7 format. The GTA may be designated in terms of an individual address (i.e., single value) or a range of addresses.

RJ-8  [534] The STP shall permit the provisioning of the following data item for each GTA Reference/GTA data combination uniquely provisioned when one or more GTAs are to be mapped to a specific set of ordered DPC data as defined by the Ordered DPC Translation data.

...  Ordered DPC Reference - alphanumeric(8), variable length; identifies a set of translation data in the Ordered DPC Translation data that should be used by the GTT process. The special argument “V” may be specified for the Ordered DPC Reference to denote an intentionally vacant GTA code for which there is no valid GTT as described in Section 4.3.1.1.

RJ-9  [535] The STP shall permit the provisioning of the following data items for each GTA Reference/GTA data combination uniquely provisioned when one or more GTAs are to be mapped to a specific DPC or capability code or to indicate vacant GTA codes:

...  Destination Point Code (DPC) - numeric(9) or alphabetic (1), fixed length; identifies the DPC which is to be provided by the STP in the translated message’s routing label as the result of the GTT. This attribute may contain the DPC of a specific signaling point (e.g., an SCP hosting database applications or a CCS switching office/SSP hosting signaling applications)
or a capability code referring to a pair or set of STPs that will perform a subsequent GTT. This attribute is formed by the concatenation of the three base-10 (decimal) representations of the corresponding binary octets comprising the network identifier (NI), network cluster (NC), and network cluster member (NCM) subfields of the internally stored binary DPC or capability code. Valid NIs and NCs are 001 through 255. Valid NCMs are 000 through 255. In addition, the special argument “V” may be specified for the DPC to denote an intentionally vacant GTA code for which there is no valid GTT as described in Section 4.3.1.1.

Routing Indicator (RI) - alphanumeric(1), fixed length; identifies whether subsequent routing should be based on the GT in the CdPA (i.e., a GTT is required) or based on the DPC in the routing label and SSN in the CdPA (i.e., a GTT is not required). This attribute is the decimal representation of the 1-bit binary field in the address indicator used in the SS7 protocol to identify the routing indicator. Valid routing indicators are 0 or 1. In addition, the special argument “V” may be specified for the RI to denote an intentionally vacant GTA code for which there is no valid GTT as described in Section 4.3.1.1.

Override SSN - numeric(3) or alphabetic (1), fixed length; the identification of the application software subsystem that should process SS7 messages, as previously defined in Item A for the SSN data item. In addition, the special argument “V” may be specified for the override SSN to denote an intentionally vacant GTA code for which there is no valid GTT as described in Section 4.3.1.1. A null override SSN indicates the SSN defined in the TT-to-SSN Mapping Translation data will be used for the GTT function. A non-null override SSN indicates the override SSN will be used for the GTT function.

Remarks - alphanumeric(20), variable length; a user-specified comment field that may be used to provide a brief description of the objective/purpose of the GTT to be performed.

C. Multi-Step GTT: Ordered DPC Translation

The STP shall permit the provisioning of Ordered DPC Translation data to identify the set of ordered DPCs that should be used in the GTT process. Each DPC will be associated with a routing indicator and relative
cost that will be used to indicate the routing preference for the SS7 message.

**RJ-13** [539] The STP shall permit the provisioning of the following data items for Ordered DPC Translation data:

... *Ordered DPC Reference* - alphanumeric(8); variable length; identifies one or more DPC data combinations that should be used in the GTT process.

... *Relative Cost* - numeric(2), fixed length; the weighting factor applied to the DPC data combination. The costs will be assigned values from 00 to 99, representing the most desirable to the least desirable, respectively. In general, if there are 2 or more DPCs defined, the DPC with the lowest relative cost should be selected. If the selected DPC is unavailable (i.e., inaccessible), the DPC with the next lowest cost should be selected.

... *Destination Point Code (DPC)* - numeric(9), fixed length; identifies the DPC which is to be provided by the STP in the translated message’s routing label as the result of the GTT. This attribute should contain the DPC of a specified SCP hosting a replicated data-based application or the capability code of an STP that will perform a subsequent GTT for the message. This attribute is formed by the concatenation of the three base-10 (decimal) representations of the corresponding binary octets comprising the network identifier (NI), network cluster (NC), and network cluster member (NCM) subfields of the internally stored binary DPC or capability code. Valid NIs and NCs are 001 through 255. Valid NCMs are 000 through 255.

... *Routing Indicator (RI)* - alphanumeric(1), fixed length; identifies whether subsequent routing should be based on the GT in the CdPA (i.e., a GTT is required) or based on the DPC in the routing label and SSN in the CdPA (i.e., a GTT is not required). This attribute is the decimal representation of the 1-bit binary field in the address indicator used in the SS7 protocol to identify the routing indicator. Valid routing indicators are 0 or 1.

**CRJ-14** [540] As a per-Bcc option, the STP shall permit the provisioning of the following data item for Ordered DPC Translation data:

... *Override SSN* - numeric(3), fixed length; the identification of the application software subsystem that should process SS7 messages, as previously defined in Item A for the SSN data item. A null override SSN indicates the SSN defined in the TT-to-SSN Mapping Translation data will be used for the GTT function. A non-null override SSN indicates the SSN defined in the Ordered DPC Translation data will be used for the GTT function.

---

2 DPCs assigned equal cost indicates SCCP loadsharing.
OJ-15  [541] It is desirable that the STP permit the provisioning of the following data item for each Ordered DPC Reference/Relative Cost/DPC data combination:

...  
Remarks - alphanumeric(20), variable length; a user-specified comment field that may be used to provide a brief description of the objective/purpose of the GTT to be performed.

J.1.2.2  Data Operations

Following are the RC&V command actions that are required to support the provisioning of GTT data at STPs.

A.  *Multi-Step GTT: TT-to-SSN Mapping Translation*

   RJ-16  [542] The STP shall permit the RC&V command actions described below to support the TT-to-SSN Mapping Translation provisioning data:

   ...  
   • Add, Delete, and Verify a TT, SSN, and GTA reference
   ...  
   • Change an SSN or GTA reference for a given TT.

   OJ-17  [543] It is desirable that the STP permit the RC&V command action described below to support the TT-to-SSN Mapping Translation provisioning data:

   ...  
   • Add, Delete, Change, and Verify the remarks for a given TT.

B.  *Multi-Step GTT: GTA-to-DPC Mapping Translation*

   RJ-18  [544] The STP shall permit the RC&V command actions described below to support the GTA-to-DPC Mapping Translation provisioning data:

   ...  
   • Add, Delete, and Verify a GTA reference, GTA, Ordered DPC reference, DPC, and RI
   ...  
   • Change a GTA, Ordered DPC reference, DPC, or RI for a given GTA reference and GTA.

   CRJ-19  [545] As a per-Bcc option, the STP shall permit the RC&V command actions described below to support the GTA-to-DPC Mapping Translation provisioning data:

   ...  
   • Add, Delete, and Verify a GTA reference, GTA, ordered DPC reference, DPC, override SSN, and RI
   ...  
   • Change a GTA, ordered DPC reference, DPC, override SSN, or RI for a given GTA reference and GTA.
OJ-20 [546] It is desirable that the STP permit the RC&V command action described below to support the GTA-to-DPC Mapping Translation provisioning data:

…

• Add, Delete, Change, and Verify the remarks for a given GTA reference and GTA.

C. Multi-Step GTT: Ordered DPC Translation

RJ-21 [547] The STP shall permit the RC&V command actions described below to support the Ordered DPC Translation provisioning data:

…

• Add, Delete, and Verify ordered DPC reference, relative cost, RI, and DPC

…

• Change a relative cost, RI, or DPC for a given ordered DPC reference, relative cost, RI, and DPC.

CRJ-22 [548] As a per-Bcc option, the STP shall permit the RC&V command actions described below to support the Ordered DPC Translation provisioning data:

…

• Add, Delete, and Verify ordered DPC reference, relative cost, RI, DPC, and override SSN

…

• Change a relative cost, RI, DPC, or override SSN for a given ordered DPC reference, relative cost, RI, and DPC.

OJ-23 [549] It is desirable that the STP permit the RC&V command action described below to support the Ordered DPC Translation provisioning data:

…

• Add, Delete, Change, and Verify the remarks for a given ordered DPC reference, relative cost, RI, and DPC.

D. Multi-Step GTT: Ordered GTT Translation Verify

RJ-24 [550] The STP shall permit the following Verify command action to support the provisioning of multi-step GTT data:

…

• Verify a DPC, SSN, RI, and relative cost for a specified GTA and TT.

J.1.2.3 Database Management Functions

RJ-25 [551] The provisioning data shall be supported with the database management functions described in the OTGR Section 2.1: Memory Administration.
J.1.3 Surveillance Requirements

Surveillance measurement requirements to support GTT data are provided in the following sub-sections of Section 6 (STP Performance Management):

- Section 6.4.2 (System Total Measurements)
- Section 6.4.3 (Translation Type Measurements).

Surveillance event notification requirements to support GTT data are provided in the following sub-sections of Section 6 (STP Performance Management):

- Section 6.6.2 (Event Report Types).

J.2 Operations Requirements for UDT/XUDT Message Processing

This section provides the operations requirements that are needed to identify the applications in the CCS network that are recognized by the STP and to support the STP procedures that route UDT/XUDT messages to the applications.

J.2.1 Overview

To support UDT/XUDT message processing, SCCP application data is required to be provisioned at the STP. SCCP application data is specifically needed to support multi-step GTT procedures, signaling point congestion control, and ISNI message processing and will be used as follows:

- to verify that the DPC and SSN that result from a GTT, and to which a message will be routed, is valid (i.e., the SSN is supported at the DPC) [see Section 4.3.1.1]
- to specify whether or not the STP should redirect traffic to the next preferred subsystem when congestion is encountered when routing to the preferred subsystem [see Section 4.3.3.2.1]
- to verify whether or not an application is ISNI capable [see Appendix E, Section E.5].

In general, SCCP application data will be used to identify the applications, in the form of a DPC and SSN, that are equipped at the signaling points to which the STP routes message traffic. Each DPC and SSN provisioned will be associated with certain parameters that are used to support the processing of UDT/XUDT messages. The Alternate-Routing-On-Congestion indicator associated with SCCP application data will be used to specify whether

3. A previous description of SCCP application data included an XUDT Capability Indicator to indicate whether the application at the node supports the processing of XUDT messages. This attribute has been deleted from the SCCP application data and moved to the Destination data as described in Section 5 since an indication of XUDT capability is more accurately represented on a per-destination basis rather than a per-application basis.
or not the STP should redirect traffic to the next preferred subsystem when congestion is encountered when routing to the preferred subsystem (see Section 4.3.3.2.1). The ISNI Capability indicator associated with SCCP application data will be used to verify whether or not an application is ISNI capable (see Appendix E, Section E.5). Default values associated with these parameters may be used by the STP if these parameters are not explicitly provisioned. As a per-Bcc option, other parameters may also be provisioned to reference a reusable list of concerned signaling points to which SCCP management messages will be broadcasted (Concerned Signaling Point List Reference) and to provide an alternative method for identifying applications according to their geographic location or relationship (Application Identifier).

### J.2.2 Provisioning Requirements

#### J.2.2.1 Provisioning Data Elements

This section provides a detailed description of the provisioning data that is required to support the provisioning of SCCP application data at the STP.

**RJ-26** [552] The STP shall permit the provisioning of SCCP application data to identify the applications in the CCS network that are recognized by the STP’s SCCP procedures, to control alternate routing during congestion, and to identify those applications that are ISNI capable.

**RJ-27** [553] The STP shall permit the provisioning of the following data items for SCCP application data:

- **Destination Point Code (DPC)** - numeric(9), fixed length; the DPC at which the application resides. This attribute is formed by the concatenation of the three base-10 (decimal) representations of the corresponding binary octets comprising the network identifier (NI), network cluster (NC), and network cluster member (NCM) subfields of the internally stored binary signaling point code.

- **Subsystem Number (SSN)** - numeric(3), fixed length; the identification of the specific application software subsystem at the signaling point identified by the DPC above. This attribute is comprised of the decimal representation of the binary number in the 1-octet field used by the SS7 protocol. Valid SSNs values include 000 and the range from 002 through 255 (NOTE: The value 001 is reserved for SCCP management messages). The value 000 shall be used to denote the SCCP function at a subsequent STP capable of performing intermediate GTTs and ISNI translations (i.e., an STP’s SCCP functions shall be regarded as the 000 subsystem at the target STP).
RJ-28  [554] The STP shall permit the provisioning of the following data items for each DPC/SSN data combination uniquely provisioned:

…  **Alternate-Routing-On-Congestion Indicator** - numeric(1), fixed length; indicates whether the STP should redirect traffic to the next preferred subsystem when congestion is encountered towards the point code corresponding to the preferred subsystem identified by the DPC/SSN data combination defined above. Valid alternate-routing-on-congestion indicators are: 0 or 1. A value of 1 is applicable only for replicated applications for which alternate applications are specified in the GTT data and indicates that the STP should reroute traffic to the next preferred subsystem. A value of 0 indicates either the STP should not reroute traffic (for replicated applications) or rerouting does not apply (for non-replicated applications). The value of 0 shall be the default value.

…  **ISNI Capability Indicator** - numeric(1), fixed length; indicates whether the application at the node identified by the DPC/SSN data combination defined above supports the ISNI capability. Valid ISNI Capability Indicators are: 0 or 1. A value of 0 indicates that the application does not support ISNI and a value of 1 indicates that the application does support ISNI. The value of 1 shall be the default value.

CRJ-29  [555] As a per-Bcc option, the STP shall permit the provisioning of the following data items for each DPC/SSN data combination uniquely provisioned:

…  **Concerned Signaling Point List Reference** - alphanumeric (9), first character alphabetic, variable length; a reference to a reusable list of concerned signaling points to which SSP and SSA SCCP management messages shall be broadcast upon receipt of SSPs/SSAs concerning the indicated application. It shall enable CSP lists to be reused across applications. When a reference is specified, the STP should refer to a list of concerned SPs provisioned for that reference in the Concerned Signaling Point data defined in Section 5. When null, this parameter conveys that the STP should check for a list of concerned signaling points based on the DPC-SSN of the Concerned Signaling Point data defined in Section 5, or if no such list of concerned signaling points are found, that the SSP/SSA broadcast is not applicable. A null value must be specified if the SSN attribute is 000 (i.e., the application corresponds to an STP). It is important to note that more than one reference may be provisioned.

…  **Application Identifier** - alphanumeric/graphic(16), variable length; the mnemonic identifier to refer to the given target SCCP application subsystem or STP pair. It may be used to denote the location of the signaling point and the type of application subsystem. In order to allow remote subsystems or gateway STP pairs to be associated according to
their geographic location or relationship, or to identify their owner or network operator, the STP shall support the assignment of the same application identifier to multiple application subsystems or signaling points.

J.2.2.2 Data Operations

Following are the RC&V command actions that are required to support the provisioning of SCCP application data at STPs.

**RJ-30 [556]** The STP shall permit the RC&V command actions described below to support the SCCP application provisioning data:

- Add, Delete, and Verify a DPC, SSN, alternate-routing-on-congestion indicator, and ISNI capability indicator
- Change an alternate-routing-on-congestion indicator or ISNI capability indicator for a given DPC/SSN.

**CRJ-31 [557]** As a per-Bcc option, the STP shall permit the RC&V command actions described below to support the SCCP application provisioning data:

- Add, Delete, and Verify a DPC, SSN, alternate-routing-on-congestion indicator, ISNI capability indicator, concerned signaling point list reference and application identifier
- Change an alternate-routing-on-congestion indicator, ISNI capability indicator, concerned signaling point list reference or application identifier for a given DPC/SSN.

J.2.2.3 Database Management Functions

**RJ-32 [558]** The provisioning data shall be supported with the database management functions described in the OTGR: Network Element Memory Administration.

J.2.3 Surveillance Requirements

No surveillance requirements are needed at this time.
References

Bellcore Documents


3. **TA-TSY-000077**, *Digital Channel Banks Requirements for Dataport Channel Unit Functions*, Issue 3 (Bellcore, April 1986).


11. **GR-376-CORE**, *OTGR Section 15.3: Generic Operations Interfaces Using OSI Tools: Network Data Collection (NDC)* (a module of OTGR, FR-439), Issue 2, (Bellcore, September 1996); plus revisions.


15. **GR-454-CORE**, *Generic Requirements for Supplier-Provided Documentation* (a module of LSSGR, FR-64; TSGR, FR-440; and OTGR, FR-439), Issue 1 (Bellcore, December 1997).


20. **GR-478-CORE**, *OTGR Section 8: Measurements and Data Generation* (a module of OTGR, FR-439, and LSSGR, FR-64), Issue 3 (Bellcore, December 1997); plus Revision 1, July 1998.


23. **GR-506-CORE**, *LSSGR: Signaling for Analog Interfaces* (a module of LSSGR, FR-64), Issue 1 (Bellcore, June 1996); plus Revision 1, November 1996.

24. **TR-TSY-000510**, *LSSGR: System Interfaces, Section 10* (a module of LSSGR, FR-64), Issue 2 (Bellcore, July 1987); plus revisions.


27. **TR-NWT-000533**, *Database Services-Service Switching Points, FSD 31-01-0000* (a module of LSSGR, FR-64), Issue 3 (Bellcore, January 1994); plus Supplement 1, April 1995.


34. **GR-828-CORE**, *OTGR Section 11.2: Generic Operations Interface - OSI Communications Architecture* (a module of OTGR, FR-439), Issue 1 (Bellcore, September 1994); plus Revision 1, October 1996.


36. **GR-839-CORE**, *Generic Requirements for Supplier Provided Training* (a module of LSSGR, FR-64; OTGR, FR-439; and TSGR, FR-440), Issue 1 (Bellcore, July 1996).

37. **TR-NWT-000840**, *Supplier Support Generic Requirements (SSGR)* (a module of LSSGR, FR-64; TSGR, FR-440; and OTGR, FR-439), Issue 1 (Bellcore, December 1991).

38. **GR-874-CORE**, *An Introduction to the Reliability and Quality Generic Requirements (RQGR)*, Issue 3 (Bellcore, April 1997).


42. **TR-NWT-001372**, *Generic Requirements for Enhanced SS7 Message Trapping Capabilities*, Issue 1 (Bellcore, November 1993).


45. **GR-2932-CORE**, *Database Functionalities* (a module of LSSGR, FR-64), Issue 1 (Bellcore, May 1997).

**Note:**

All Bellcore documents are subject to change, and their citation in this document reflects the most current information available at the time of this printing. Readers are advised to check current status and availability of all documents.

**To Contact Bellcore**

Bellcore Customer Service  
8 Corporate Place, Room 3A-184  
Piscataway, New Jersey 08854-4156  
1-800-521-CORE (2673) (USA and Canada)  
1 (732) 699-5800 (all others)  
1 (732) 336-2559 (FAX)

**To Order Documents**

- Perform the following steps to order from the online catalog:
  1. Enter the URL line: *telecom-info.bellcore.com*
  2. Click on the *Search* button located on top
  3. In the *Keywords* field, enter the document number (or keywords), then click on *Submit Search*.
  
  or

  1. Enter the above URL line
  2. Click on the *Browse* button located on top, then click on the subject of interest.

- Bellcore employees should perform the following steps:
  1. Access the Bellcore Internal Home Page
  2. Click on the *Marketwise* button located on top
  3. Click on *DOCS - Bellcore Product Catalog*
  4. Enter data in one or more of the fields (e.g., enter a document number in the *Product Number* field), then follow the instructions to search the online catalog.
Other Documents


CCITT Recommendation X.25

## Glossary

### Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>Bcc</td>
<td>Bellcore client company</td>
</tr>
<tr>
<td>BIB</td>
<td>Backward Indicator Bit</td>
</tr>
<tr>
<td>CC</td>
<td>Composite Clock</td>
</tr>
<tr>
<td>CCS</td>
<td>Common Channel Signaling</td>
</tr>
<tr>
<td>CCSSO</td>
<td>Common Channel Signaling Switching Office</td>
</tr>
<tr>
<td>CO</td>
<td>Central Office</td>
</tr>
<tr>
<td>CRM</td>
<td>Cluster Routing Management</td>
</tr>
<tr>
<td>CRMD</td>
<td>Cluster Routing and Management Diversity</td>
</tr>
<tr>
<td>CRT</td>
<td>Cathode Ray Tube</td>
</tr>
<tr>
<td>CSU</td>
<td>Channel Service Unit</td>
</tr>
<tr>
<td>DCE</td>
<td>Data Circuit Terminating Equipment</td>
</tr>
<tr>
<td>DDS</td>
<td>Digital data System</td>
</tr>
<tr>
<td>DF</td>
<td>Distributing Frame</td>
</tr>
<tr>
<td>DPC</td>
<td>Destination Point Code</td>
</tr>
<tr>
<td>DSU</td>
<td>Data Service Unit</td>
</tr>
<tr>
<td>DSX</td>
<td>Digital Systems Cross-connect Frame</td>
</tr>
<tr>
<td>DTE</td>
<td>Data Terminal Equipment</td>
</tr>
<tr>
<td>ECSA</td>
<td>Exchange Carriers Standards Association</td>
</tr>
<tr>
<td>EIA</td>
<td>Electronic Industries Association</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FIB</td>
<td>Forward Indicator Bit</td>
</tr>
<tr>
<td>FISU</td>
<td>Fill-in Signal Unit</td>
</tr>
<tr>
<td>FSD</td>
<td>Feature Specific Document</td>
</tr>
<tr>
<td>GTT</td>
<td>Global Title Translation</td>
</tr>
<tr>
<td>I/O</td>
<td>Input/Output</td>
</tr>
<tr>
<td>ISDN</td>
<td>Integrated Services Digital Network</td>
</tr>
<tr>
<td>ISDNUP</td>
<td>Integrated Services Digital Network User Part</td>
</tr>
<tr>
<td>ISNI</td>
<td>Intermediate Signaling Network Identification</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organization</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>LATA</td>
<td>Local Access and Transport Area</td>
</tr>
<tr>
<td>LIDB</td>
<td>Line Information Database</td>
</tr>
<tr>
<td>LSSGR</td>
<td>LATA Switching Systems Generic Requirements</td>
</tr>
<tr>
<td>LSTP</td>
<td>Local Signaling Transfer Point</td>
</tr>
<tr>
<td>MML</td>
<td>Human-Machine Language</td>
</tr>
<tr>
<td>MSU</td>
<td>Message Signal Unit</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time Between Failures</td>
</tr>
<tr>
<td>MTP</td>
<td>Message Transfer Part</td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time To Repair</td>
</tr>
<tr>
<td>OA&amp;M</td>
<td>Operations, Administration, and Maintenance</td>
</tr>
<tr>
<td>OMAP</td>
<td>Operations, Maintenance, and Administration Part</td>
</tr>
<tr>
<td>OPC</td>
<td>Originating Point Code</td>
</tr>
<tr>
<td>OS</td>
<td>Operations System</td>
</tr>
<tr>
<td>OSI</td>
<td>Open System Interconnection</td>
</tr>
<tr>
<td>OSN</td>
<td>Operations Systems Network</td>
</tr>
<tr>
<td>OSS</td>
<td>Operator Services System</td>
</tr>
<tr>
<td>OTGR</td>
<td>Operations Technology Generic Requirements</td>
</tr>
<tr>
<td>PC</td>
<td>Point Code</td>
</tr>
<tr>
<td>PCR</td>
<td>Preventive Cyclic Retransmission</td>
</tr>
<tr>
<td>PPSN</td>
<td>Public Packet Switched Network</td>
</tr>
<tr>
<td>QPA</td>
<td>Quality Program Analysis</td>
</tr>
<tr>
<td>R&amp;Q</td>
<td>Reliability and Quality</td>
</tr>
<tr>
<td>RC</td>
<td>Recent Change</td>
</tr>
<tr>
<td>RC&amp;V</td>
<td>Recent Change and Verify</td>
</tr>
<tr>
<td>RCP</td>
<td>Cluster-Route-Set-Test-Prohibited</td>
</tr>
<tr>
<td>RCR</td>
<td>Cluster-Route-Set-Test-Limited</td>
</tr>
<tr>
<td>RCT</td>
<td>Route-Set-Congestion-Test</td>
</tr>
<tr>
<td>RSP</td>
<td>Route-Set-Prohibited message</td>
</tr>
<tr>
<td>RSR</td>
<td>Route-Set-Limited message</td>
</tr>
<tr>
<td>RSTP</td>
<td>Regional Signaling Transfer Point</td>
</tr>
<tr>
<td>SCCP</td>
<td>Signaling Connection Control Part</td>
</tr>
<tr>
<td>SCCS</td>
<td>Signaling Control Center System</td>
</tr>
<tr>
<td>SCP</td>
<td>Service Control Point</td>
</tr>
<tr>
<td>SEP</td>
<td>Signaling End Points</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>SI</td>
<td>Service Indicator</td>
</tr>
<tr>
<td>SIF</td>
<td>Signaling Information Field</td>
</tr>
<tr>
<td>SIO</td>
<td>Service Information Octet</td>
</tr>
<tr>
<td>SIPO</td>
<td>Signal Units Indicating Processor Outage</td>
</tr>
<tr>
<td>SLC</td>
<td>Signaling Link Code</td>
</tr>
<tr>
<td>SLS</td>
<td>Signaling Link Selection</td>
</tr>
<tr>
<td>SP</td>
<td>Signaling Point</td>
</tr>
<tr>
<td>SPC</td>
<td>Signaling Point Code</td>
</tr>
<tr>
<td>SPCS</td>
<td>Stored Program Control System</td>
</tr>
<tr>
<td>SS7</td>
<td>Signaling System Number 7</td>
</tr>
<tr>
<td>SSN</td>
<td>Subsystem Number</td>
</tr>
<tr>
<td>SSP</td>
<td>Service Switching Point</td>
</tr>
<tr>
<td>STP</td>
<td>Signaling Transfer Point</td>
</tr>
<tr>
<td>SU</td>
<td>Signal Unit</td>
</tr>
<tr>
<td>TA</td>
<td>Technical Advisory</td>
</tr>
<tr>
<td>TCA</td>
<td>Transfer-Cluster-Allowed</td>
</tr>
<tr>
<td>TCAP</td>
<td>Transaction Capabilities Application Part</td>
</tr>
<tr>
<td>TCP</td>
<td>Transfer-Cluster-Prohibited message</td>
</tr>
<tr>
<td>TCR</td>
<td>Transfer-Cluster-Restricted message</td>
</tr>
<tr>
<td>TCA</td>
<td>Transfer-Cluster-Allowed message</td>
</tr>
<tr>
<td>TFA</td>
<td>Transfer-Allowed message</td>
</tr>
<tr>
<td>TFC</td>
<td>Transfer-Controlled</td>
</tr>
<tr>
<td>TFP</td>
<td>Transfer-Prohibited message</td>
</tr>
<tr>
<td>TFR</td>
<td>Transfer-Restricted message</td>
</tr>
<tr>
<td>TR</td>
<td>Technical Reference</td>
</tr>
<tr>
<td>TRA</td>
<td>Traffic Restart Allowed</td>
</tr>
<tr>
<td>TRW</td>
<td>Traffic Restart Waiting</td>
</tr>
<tr>
<td>TSC/RTU</td>
<td>Test System Controller/Remote Test Unit</td>
</tr>
<tr>
<td>TSG</td>
<td>Timing Signal Generator</td>
</tr>
<tr>
<td>TTY</td>
<td>Teletype Terminal Unit</td>
</tr>
</tbody>
</table>
### Definitions of Terms

<table>
<thead>
<tr>
<th>Acronym/Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access key</td>
<td>A field in a database record that can be used to retrieve the record</td>
</tr>
<tr>
<td>BX.25</td>
<td>A protocol based on the CCITT X.25 protocol</td>
</tr>
<tr>
<td>CCS</td>
<td>Common Channel Signaling, an out-of-band method of signaling</td>
</tr>
<tr>
<td>CCSSO</td>
<td>A switch equipped with the ISDNUP of SS7 and possibly CLASS</td>
</tr>
<tr>
<td>Changeback</td>
<td>A procedure for diverting signaling traffic to a data link that was</td>
</tr>
<tr>
<td></td>
<td>previously out of service</td>
</tr>
<tr>
<td>CLLI code</td>
<td>An 11-character designation of equipment used in Bccs</td>
</tr>
<tr>
<td>Combined link set</td>
<td>A collection of link sets, all of which have equal desirability in</td>
</tr>
<tr>
<td></td>
<td>routing to a CCS destination</td>
</tr>
<tr>
<td>CRT</td>
<td>Cathode ray tube terminal device; also known as keyboard display or video</td>
</tr>
<tr>
<td></td>
<td>display terminal</td>
</tr>
<tr>
<td>Datagram</td>
<td>A type of message defined in X.25 that contains all addressing required</td>
</tr>
<tr>
<td></td>
<td>for routing and does not depend on a logical connection being established</td>
</tr>
<tr>
<td>DCE</td>
<td>Data circuit terminating equipment; the interface to a carrier’s network</td>
</tr>
<tr>
<td>DPC</td>
<td>Destination point code; an address used in the SS7 protocol</td>
</tr>
<tr>
<td>DTE</td>
<td>Data terminal equipment; may refer to a computer or terminal</td>
</tr>
<tr>
<td>ECSA</td>
<td>Exchange Carriers Standards Association; a North American standards group</td>
</tr>
<tr>
<td>FSD</td>
<td>Feature specific document; documents appended to the LSSGR, containing</td>
</tr>
<tr>
<td></td>
<td>requirements that are mostly independent of other switching functions or</td>
</tr>
<tr>
<td></td>
<td>most likely to change</td>
</tr>
<tr>
<td>Inband</td>
<td>A method of signaling that uses the same facilities that are used for the</td>
</tr>
<tr>
<td></td>
<td>call</td>
</tr>
<tr>
<td>ISDNUP</td>
<td>Integrated services digital network user part; a component part of the</td>
</tr>
<tr>
<td></td>
<td>SS7 protocol</td>
</tr>
<tr>
<td>Link set</td>
<td>A collection of CCS links, all of which terminate on the same two</td>
</tr>
<tr>
<td></td>
<td>signaling points</td>
</tr>
<tr>
<td>MML</td>
<td>Human-machine language; a CCITT specification for the human-machine</td>
</tr>
<tr>
<td></td>
<td>interface</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean time between failures; a measure of availability</td>
</tr>
<tr>
<td>MTP</td>
<td>Message transfer part; a component part of the SS7 protocol</td>
</tr>
</tbody>
</table>

Glossary–4
<table>
<thead>
<tr>
<th>Acronym/Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTTR</td>
<td>Mean time to repair; a measure of availability</td>
</tr>
<tr>
<td>OA&amp;M</td>
<td>Operations, administration, and maintenance; a component of the SS7 protocol that specifies procedures and measurements for managing the CCSS network</td>
</tr>
<tr>
<td>OPC</td>
<td>Originating point code; an address used in SS7 protocol</td>
</tr>
<tr>
<td>OSI</td>
<td>Open systems interconnection; a model for data networks proposed by ISO</td>
</tr>
<tr>
<td>OSN</td>
<td>Operation system network; OC data communications network used for interactions between operations support systems, telecommunications equipment, and Bcc data terminal users</td>
</tr>
<tr>
<td>RC&amp;V</td>
<td>Recent change and verify; a function in the STP that enables changes to STP-resident data and allows verification of data</td>
</tr>
<tr>
<td>RS-232-C</td>
<td>Standard interfaces between a modem and DTE specified by the Electronic Industries Association</td>
</tr>
<tr>
<td>RS-449</td>
<td></td>
</tr>
<tr>
<td>SCCP</td>
<td>Signaling connection control part; a component part of SS7 protocol</td>
</tr>
<tr>
<td>SCCS</td>
<td>Switching control center system; a maintenance operations system</td>
</tr>
<tr>
<td>SCP</td>
<td>Service control point; transaction processor-based system that provides network interface to database services</td>
</tr>
<tr>
<td>SEAS</td>
<td>Signaling Engineering and Administration System; an operations support system for the CCS network</td>
</tr>
<tr>
<td>SIF</td>
<td>Signaling information field; the field in SS7 messages that contains data from user parts</td>
</tr>
<tr>
<td>SIO</td>
<td>Service information octet; a filed in SS7 messages that directs the signal unit to the appropriate user part</td>
</tr>
<tr>
<td>SLC</td>
<td>Signaling link code; an SS7 identifier of a signaling link, which is unique within a link set and is held in common between two signaling points that terminate the link</td>
</tr>
<tr>
<td>SLS</td>
<td>Signaling link selection; a parameter that is part of the routing label within the SIF</td>
</tr>
<tr>
<td>SP</td>
<td>Signaling point; a node in the CCS network</td>
</tr>
<tr>
<td>SS7</td>
<td>Signaling System Number 7; the protocol specified internationally by CCITT Study Group XI/2 and domestically by the ECSA T1X1.1 Working Group</td>
</tr>
<tr>
<td>SSN</td>
<td>Subsystem number; an address used in the SCCP of SS7 to designate an application at an end signaling point</td>
</tr>
<tr>
<td>SSP</td>
<td>Service switching point; a switching office that has the SSP features, enabling interactions with SCPs to provide services and routing</td>
</tr>
<tr>
<td>Acronym/Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>STP</td>
<td>Signaling transfer point; the packet switch in the CCS network that transfers messages from one signaling link to another at Level 3</td>
</tr>
<tr>
<td>T1X1.1</td>
<td>The working group within the ECSA’s T1 (telephone) Committee that is responsible for U.S. CCS standards</td>
</tr>
<tr>
<td>TC</td>
<td>Transaction capability; a part of the SS7 protocol used for database services</td>
</tr>
<tr>
<td>TTY</td>
<td>Teletype terminal unit, teletypewriter equipment</td>
</tr>
</tbody>
</table>