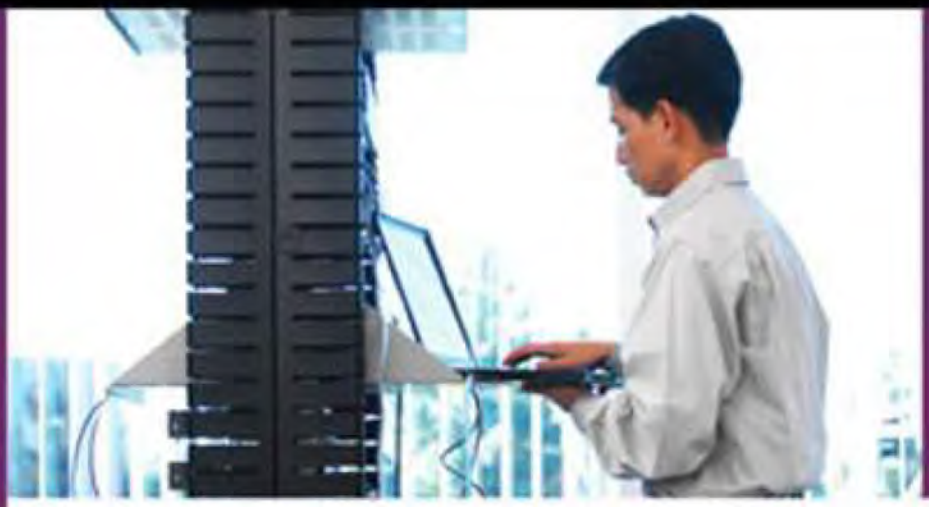
Cisco Systems



IP COMMUNICATIONS

Signaling System No. 7 (SS7/C7)

Protocol, Architecture, and Services

A complete, practical guide to the world's most popular signaling system, including SIGTRAN, GSM-MAP, and Intelligent Networks

Lee Dryburgh
Jeff Hewett

ciscopress.com

GOOGLE EXHIBIT 1011 (Part 1 of 5)

Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services

Lee Dryburgh
Jeff Hewett

Cisco Press

800 East 96th Street
Indianapolis, IN 46240 USA

Signaling System No. 7 (SS7/C7):
Protocol, Architectures, and Services

Lee Dryburgh
Jeff Hewett

Copyright © 2005 Cisco Systems, Inc.

Published by:
Cisco Press
800 East 96th Street
Indianapolis, Indiana 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

First Printing June 2005

Library of Congress Cataloging-in-Publication Number: 2001090446

ISBN: 1-58705-040-4

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

This book is designed to provide information about Signaling System No. 7 and related technologies. Every effort has been made to make this book as complete and accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

Corporate and Government Sales

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact:

U.S. Corporate and Government Sales: 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside of the U.S. please contact: international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members of the professional technical community.

Reader feedback is a natural continuation of this process. If you have any comments about how we could improve the quality of this book or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please be sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher	John Wait
Editor-in-Chief	John Kane
Cisco Press Program Manager	Nanette M. Noble
Cisco Marketing Program Manager	Edie Quiroz
Acquisitions Editor	Amy Moss
Managing Editor	Patrick Kanouse
Development Editor	Jennifer Foster
Technical Editors	Franck Noel, Brad Dunsmore, Trevor Graham, Andreas Nikas, Jan Van Geel, Murry Gavin
Project Editor	Marc Fowler
Copy Editors	Bridget Collins, Gayle Johnson
Team Coordinator	Tammi Barnett
Book and Cover Designer	Louisa Adair
Production Team	Octal Publishing, Inc.
Indexers	Larry Sweazy Tim Wright

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Net Readiness Scorecard, Networking Academy, and ScriptShare are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

Printed in the USA

About the Authors

Lee Dryburgh, BSc MIEE, is a specialist in SS7/C7 and the services it empowers. He provides training and consulting through his company, Bit Tech Limited. His entire career has focused on SS7/C7. He has uniquely tackled the subject from many career positions, including software engineering, testing, training, security auditing, and architectural design, in both fixed-line and cellular networks. He is a member of several professional telecommunications bodies and holds a degree in computer science. He is currently studying for an engineering doctorate at the University College of London. He can be reached at lsd@bittech.co.uk. He very much welcomes specific feedback about this book. Such comments can be addressed to him at book@c7.com.

Jeff Hewett is a technical leader at Cisco Systems and is currently working in Voice over IP software development for the Government Systems Business Unit. Having been involved with SS7 for more than 16 years, he has worked in SS7 software development, testing, and training. He is a patent holder in SS7-related software development and has written about SS7 in popular journals. He has provided a broad range of SS7 training for Regional Bell Operating Companies, independent operators, and telecommunications vendors dating back to the initial rollout of SS7 in the U.S. network. In recent years, Jeff has been involved with Operating System development and Voice over Packet solutions as an engineer in the Cisco Networked Solutions Integration Test Engineering (NSITE) lab. Prior to joining Cisco, he worked in SS7 and AIN software development for a major switching vendor. He holds degrees in science and engineering and computer information systems. You can contact him at jhewett@cisco.com.

About the Technical Reviewers

Franck Noel, CCNA, CCNP, CCIP, is a consulting systems engineer with Cisco Systems, Inc. He has been in the telecommunications industry for 13 years. Most recently he has focused on designing and deploying end-to-end packet-based integrated voice and data solutions for service provider customers. Before coming to Cisco, he was on the technical staff at AT&T Bell Labs, where he worked on switching and signaling and participated in the ITU/ANSI SS7 standards. He holds a master's degree in electrical engineering.

Brad Dunsmore is a new-product instructor in advanced services at Cisco Systems. He is responsible for designing and deploying new networks for his group. Currently he specializes in SS7 offload solutions, WAN communication, and network security. He holds a B.S. in management of information systems, and he has obtained industry certifications in MCSE+Internet, MCDBA, CCNP, CCDP, CCSP, INFOSEC, and CCSI. He recently passed his written exam for the R/S CCIE and is now working on his lab.

Trevor Graham is a seasoned professional with more than 10 years of experience in the telecommunications industry. During the last four years, he has been an interconnection consultant for Cisco Systems, focusing on the Cisco voice switching products. He is responsible for defining many of the signaling and functional requirements for the switching products that Cisco will introduce into new countries, regions, and operators. Before joining Cisco, he was European switching operations manager for a large, multinational telecommunications operator. He also owned an interconnect consultancy company that provided technical interconnection consultancy and SS7 testing services to telecom operators and vendors throughout Europe.

Andreas Nikas works for the Multiservice Voice Solutions team at Cisco Systems. He has held positions in Advanced Engineering Services (AES) and Solutions Support, all with Cisco Systems. He worked for more than four years with various signaling and switching platforms related to both voice and SS7, such as the SC 2200/PGW 2200. Previously he worked for Tekelec in the Network Switching Division as a First Office Application (FOA) and Technical Assistance Center (TAC) engineer for five years in support of the Eagle Signaling Transfer Point (STP). He also worked for the U.S. Air Force and the Department of Defense for eight years in the telecommunications field.

Murry Gavin graduated from West Liberty State College in 1971 with a bachelor's degree in electrical engineering. In the past, he has worked for Stomberg-Carlson during the development and deployment of it's first electronic common control central office; Nortel and Bell Northern Research in a variety of different positions during the development and deployment of their SP-1, DMS-10, and DMS-100 family of products; and Sprint PCS Technology and Integration Center during their nation-wide deployment of services. Murry currently works at NSITE (a Cisco affiliate) and is involved with building its VoIP lab. He has also been involved in Lawful Intercept and Land Mobile Radio projects. His hobbies include amateur radio, target shooting, and sailing.

Dedications

Lee Dryburgh: To Rhoda.

“If I have any beliefs about immortality, it is that certain dogs I have known will go to heaven, and very, very few persons.” *James Thurber*

Jeff Hewett: To Janet, who is always there to encourage me.

Acknowledgments

Lee Dryburgh: Thanks to all of those at Cisco Press for their great support—in particular, John Kane, Amy Moss, and Dayna Isley. A big hello to all of those nice people at Cisco Systems who made me most welcome during my time there, especially Nigel Townley. A big thank you to the technical reviewers for their valuable input and enthusiasm. A big thank you to Ken Morneault of Cisco Systems for his valuable contribution toward the book, especially considering the circumstances. And finally, a big thank you to Tektronix for its products and support, and in particular, to Wayne Newitts, who has the unique ability to inject humor into any situation over any medium, not to mention a strange obsession with *Star Wars* and the battle between good and evil.

Jeff Hewett: As anyone who has undertaken the task knows, writing technical books is a difficult and time-consuming effort. My first acknowledgment must be to my wife Janet, who spent many evenings alone and never complained while I worked on writing material for this book. Many thanks to the people at Cisco Press for their patience and support throughout this endeavor. Also, thanks to Ken Morneault for his contribution on SIGTRAN, given such a tight schedule. I am also grateful for all of the valuable input from our technical reviewers. And finally, I'd like to say that it has been a great experience to work with the NSITE engineering group here at Cisco, with whom I shared my SS7 knowledge and from whom I gained knowledge about data networks from the best in the business.

Contents at a Glance

Introduction xxx

Part I **Introductions and Overviews 3**

Chapter 1 The Evolution of Signaling 5

Chapter 2 Standards 27

Chapter 3 The Role of SS7 43

Chapter 4 SS7 Network Architecture and Protocols Introduction 55

Chapter 5 The Public Switched Telephone Network (PSTN) 81

Part II **Protocols Found in the Traditional SS7/C7 Stack 109**

Chapter 6 Message Transfer Part 2 (MTP2) 111

Chapter 7 Message Transfer Part 3 (MTP3) 135

Chapter 8 ISDN User Part (ISUP) 183

Chapter 9 Signaling Connection Control Part (SCCP) 227

Chapter 10 Transaction Capabilities Application Part (TCAP) 267

Part III **Service-oriented Protocols 309**

Chapter 11 Intelligent Networks (IN) 311

Chapter 12 Cellular Networks 361

Chapter 13 GSM and ANSI-41 Mobile Application Part (MAP) 383

Part IV **SS7/C7 Over IP 403**

Chapter 14 SS7 in the Converged World 405

Part V **Supplementary Topics 453**

Chapter 15 SS7 Security and Monitoring 455

Chapter 16 SS7 Testing 475

Part VI **Appendixes 517**

Appendix A MTP Messages (ANSI/ETSI/ITU) 519

Appendix B ISUP Messages (ANSI/UK/ETSI/ITU-T) 525

Appendix C SCCP Messages (ANSI/ETSI/ITU-T) 533

Appendix D TCAP Messages and Components 539

Appendix E ITU-T Q.931 Messages 543

Appendix F GSM and ANSI MAP Operations 549

Appendix G MTP Timers in ITU-T/ETSI/ANSI Applications 557

Appendix H ISUP Timers for ANSI/ETSI/ITU-T Applications 563

Appendix I GSM Mobile Country Codes (MCC) and Mobile Network Codes (MNC) 573

Appendix J ITU and ANSI Protocol Comparison 595

Appendix K SS7 Standards 599

Appendix L Tektronix Supporting Traffic 607

Appendix M Cause Values 637

Acronyms 643

References 665

Index 675

Table of Contents

Introduction xxx

Part I Introductions and Overviews 3

Chapter 1 The Evolution of Signaling 5

The History of Signaling 8
1889–1976 8
1976 to Present Day 10

Subscriber Signaling 11
Address Signals 11
Supervisory Signals 13
Tones and Announcements 13
Ringing 14
Network Signaling 15

Channel Associated Signaling 15
Address Signals 16
Multifrequency 16
Supervisory Signals 18
Single Frequency(SF) 18
Digital 20
Limitations of CAS 20
Susceptibility to Fraud 20
Limited Signaling Information 20
Inefficient Use of Resources 21

Common Channel Signaling (CCS) 21
Circuit-Related Signaling 22
Non-Circuit-Related Signaling 22
Common Channel Signaling Modes 22
Associated Signaling 22
Quasi-Associated Signaling 23
Non-Associated Signaling 24

Summary 24

Chapter 2 Standards 27

History of International Telephony Standards 28
ITU-T (Formerly CCITT) International Standards 29

Regional Standards 35
ETSI 36
3rd Generation Partnership Project 36
3rd Generation Partnership Project 2 37

National and Industry Standards 37
ANSI 37
T1 Committee 38
Telcordia (Formerly Bellcore) 38
TIA/EIA 39
ATIS 40
BSI 40
NICC 40
IETF 41

Chapter 3 The Role of SS7 43

Signaling System No. 7-Based Services 45
Telephone-Marketing Numbers 45
Televoting 46
Single Directory Number 46
Enhanced 911 46
Supplementary Services 46
Custom Local Area Signaling Services (CLASS) 47
Calling Name (CNAM) 47
Line Information Database (LIDB) 48
Local Number Portability (LNP) 48
2nd and 3rd Generation Cellular Networks 49
Short Message Service (SMS) 49
Enhanced Messaging Service (EMS) 49
Private Virtual Networks 50
Do-Not-Call Enforcement 50

Signaling System No. 7: The Key to Convergence 50
Internet Call Waiting and Internet Calling Name Services 51
Click-to-Dial Applications 51
Web-Browser-Based of Telecommunication Services 51
WLAN “Hotspot” Billing 52
Location-Based Games 52

Summary 52

Chapter 4 SS7 Network Architecture and Protocols Introduction 55

Pre-SS7 Systems 56

History of SS7 57

SS7 Network Architecture 59
- Signaling Links and Linksets 60
- Routes and Routesets 61
- Node Types 62
  - Signal Transfer Point 62
  - Service Switching Point 63
  - Service Control Point 63
- Link Types 64
  - Access Links (A Links) 64
  - Cross Links (C Links) 65
  - Bridge Links (B Links) 65
  - Diagonal Links (D Links) 66
  - Extended Links (E Links) 67
  - Fully-Associated Links (F Links) 67
- Signaling Modes 68
- Signaling Network Structure 70

SS7 Protocol Overview 72
- MTP 74
  - MTP2 74
  - MTP3 75
- TUP and ISUP 75
- SCCP 75
- TCAP 76

Summary 78

Chapter 5 The Public Switched Telephone Network (PSTN) 81

Network Topology 82

PSTN Hierarchy 83
- PSTN Hierarchy in the United States 83
  - Local Exchange Network 84
  - InterExchange Network 84
  - International Network 84
  - Service Providers 84
  - Pre-Divestiture Bell System Hierarchy 86
- PSTN Hierarchy in the United Kingdom 86

Access and Transmission Facilities 87
Lines 88
The Local Loop 88
Analog Line Signaling 89
Dialing 90
Ringing and Answer 90
Voice Encoding 90
ISDN BRI 91
Trunks 92
ISDN PRI 94

Network Timing 95

The Central Office 97
Main Distribution Frame 97
The Digital Switch 97
Switching Matrix 98
Call Processing 99
Origination 100
Digit Collection 100
Translation 101
Routing 101
Connection 102
Disconnection 102
Call Setup 102

Integration of SS7 into the PSTN 103
SS7 Link Interface 104

Evolving the PSTN to the Next Generation 105

Summary 106

Part II Protocols Found in the Traditional SS7/C7 Stack 109

Chapter 6 Message Transfer Part 2 (MTP2) 111

Signal Unit Formats 112
Fill-In Signal Units 112
Link Status Signal Units 113
Message Signal Units 114
MTP2 Overhead 114
Field Descriptions 114

Signal Unit Delimitation 115

Length Indicator 116

Signal Unit Alignment 117

Error Detection 117

Error Correction 118
Basic Error Correction 118
Sequence Numbering 119
Positive Acknowledgment 119
Negative Acknowledgment 120
Response to a Positive Acknowledgment 120
Response to a Negative Acknowledgment 120
Examples of Error Correction 121
Preventive Cyclic Retransmission 123
Forced Retransmission Cycles 125
Comparison with the Basic Error Correction Method 125

Signaling Link Initial Alignment 126
Status Indications 126
Idle 127
Not Aligned 127
Aligned 127
Proving 127
Aligned/Ready 128
In Service 128

Signaling Link Error Monitoring 130
SUERM 130
AERM 131

Processor Outage 131

Flow Control 131

Summary 132

Chapter 7 Message Transfer Part 3 (MTP3) 135

Point Codes 136
ITU-T International and National Point Codes 136
ANSI National Point Codes 137

Message Format 140
Service Information Octet 140
Signaling Information Field (SIF) 142
ITU-T Routing Label 143
ANSI Routing Label 144

Signaling Message Handling 145
Discrimination 145
Distribution 146
Routing 146
ANSI Network and Cluster Routing 147
Alias Point Code Routing 148
Message Load Sharing 148
Load Sharing and MTP3 User Parts 149
SLS in ITU-T Networks 150
SLS in ANSI Networks 151
Comparing the IP and MTP3 Protocols 152
MTP3 Message Handling Example 153

Signaling Network Management 154
Network Management Messages (H0/H1 Codes) 155
Link Management 156
Signaling Link Test Control 156
Automatic Allocation of Signaling Terminals and Links 158
Route Management 158
Transfer Restricted 160
Transfer Prohibited 161
Transfer Allowed 162
Transfer Controlled 164
Traffic Management 167
Changeover 167
Emergency Changeover 169
Time-Controlled Changeover 169
Changeback 170
Time-Controlled Diversion 170
Forced Rerouting 171
Controlled Rerouting 172
MTP Restart 173
Management Inhibiting 175
MTP3/User Part Communication 178
Signaling Network Management Example 179

Summary 181

Chapter 8 ISDN User Part (ISUP) 183

Bearers and Signaling 184

ISUP and the SS7 Protocol Stack 185
ISUP Standards and Variants 186

ISUP Message Flow 187
Call Setup 188
Call Release 188
Unsuccessful Call Attempt 189

Message Timers 189

Circuit Identification Codes 190
DPC to CIC Association 191
Unidentified Circuit Codes 192

Enbloc and Overlap Address Signaling 192
Enbloc Signaling 193
Overlap Signaling 193

Circuit Glare (Dual-Seizure) 194
Resolving Glare 195
Avoiding Glare 195

Continuity Test 196
Loopback and Transceiver Methods 196
Continuity Check Procedure 197

ISUP Message Format 198
Basic Call Message Formats 200
Initial Address Message (IAM) 200
Subsequent Address Message (SAM–ITU Networks Only) 203
Continuity Message (COT) 203
Address Complete Message (ACM) 204
Answer Message (ANM) 205
Release Message (REL) 205
Release Complete Message (RLC) 206

Detailed Call Walk-Through 206
Call Setup 206
Call Release 208
Terminal Portability 208

Circuit Suspend and Resume 208

ISUP and Local Number Portability 209
All Call Query (ACQ) 210
Query On Release (QOR) 211
Dropback (Also Known as Release to Pivot) 211
Onward Routing (OR) 211

ISUP-ISUP Tandem Calls 211
ISUP Message Processing at a Tandem 212
Continuity Testing 213
Transporting Parameters 213

Interworking with ISDN 213
End-to-End Signaling 215
ISDN Signaling Indicators in the IAM 215

Supplementary Services 216
Calling Line Identification (CLI) Example 217
Call Forwarding Example 218

Additional Call Processing Messages 220

Maintenance Messages and Procedures 220
Circuit Ranges 220
Circuit States 221
Circuit Validation (ANSI Only) 222
Continuity Testing 222
Blocking and Unblocking Circuits 223
Circuit Reset 223

Summary 224

Chapter 9 Signaling Connection Control Part (SCCP) 227

SCCP Architecture 229

SCCP Message Transfer Services 230
Connection-oriented Versus Connectionless Services 231
User Data and Segmentation 232
Connectionless Protocol Classes 232
Connection-oriented Protocol Classes 233
SCCP Connectionless Control (SCLC) 234
SCCP Connection-Oriented Control (SCOC) 234

SCCP Messages and Parameters 236
Message Structure 237
Mandatory Fixed Part (MF) 237
Mandatory Variable Part (MV) 238
Optional Part (O) 239

Message Types 240
Connection Request (CR) 240
Connection Confirm (CC) 240
Connection Refused (CREF) 241
Released (RLSD) 242
Release Complete (RLC) 242
Data Form 1 (DT1) 243
Unitdata (UDT) 243
Unitdata Service (UDTS) 244

SCCP Routing Control (SCRC) 244
Subsystem Number (SSN) Routing 245
Global Title Routing 249
Global Title Translation 249
Calling Party Address (CgPA) and Called Party Address (CdPA) 253

SCCP Management (SCMG) 260
Replicate Subsystems 261
SCMG Messages 262
Signaling Point Status Management 263
Subsystem Status Management 263

Summary 264

Chapter 10 Transaction Capabilities Application Part (TCAP) 267

Overview 268
Generic Service Interface 268
Role of TCAP in Call Control 269
TCAP Within the SS7 Protocol Stack 269
Transaction and Component Sublayers 270

Message Types 270

Transactions 272
Transaction IDs 272
Establishing Transaction IDs 273
Releasing Transaction IDs 274
Transaction Message Sequence 274

Components 276
Invoke and Return Result Components 276
Component IDs 278
Operation Codes 278

Parameters 279
ITU Parameters 280

Dialogue Portion 280
ITU Dialogue 280
ANSI Dialogue 282

Message Encoding 282

Element Structure 283
Element Identifier 284
Constructors and Primitives 284
Identifier Tag 285
Length Identifier 286
Message Layout 286

Error Handling 288
Protocol Errors 288
Errors at the Transaction Layer 288
Errors at the Component Layer 289
Application Errors 289
End-User Errors 289
Handling Application and End-User Errors 289

ITU Protocol Message Contents 290
Unidirectional Message 290
Begin Message 291
End Message 291
Continue Message 292
Abort Message 292

ANSI Protocol Message Contents 293
Unidirectional Message 293
Query With/Without Permission 294
Conversation With/Without Permission 295
Response Message 295
Protocol Abort (P-Abort) Message 296
User Abort (U-Abort) Message 296

ANSI National Operations 297

ANSI Parameters 299

Summary 306

Part III Service-oriented Protocols 309

Chapter 11 Intelligent Networks (IN) 311

The Intelligent Network 312

Service Logic and Data 312
- Service Logic 313
- Service Data 313
- Service Distribution and Centralization 314

IN Services 315

IN and the SS7 Protocol 316

Evolution of the Network 317

IN/1 319
- Initial Services 319
- IN/1 Toll-Free (E800) Example 320

The Advanced Intelligent Network (AIN 0.X, IN CS-X) 323
- Basic Call State Models (BCSM) 323
  - Point in Call (PIC) 323
  - Detection Point (DP) 324
  - Trigger Detection Point (TDP) 324
  - Event Detection Point (EDP) 325
  - Trigger and Event Precedence 326
  - Escape Codes 326
  - Originating and Terminating Call Models 327
- Network Architecture 328
  - Service Switching Point (SSP) 329
  - Service Control Point (SCP) 329
  - Adjunct 329
  - Intelligent Peripheral (IP) 329
  - Service Management System (SMS) 330
  - Service Creation Environment (SCE) 330
- ITU Intelligent Network Conceptual Model (INCM) 330
  - Correlating Distributed Functional Plane and Physical Plane 331
- AIN 0 332
- IN CS-1/AIN 0.1 333
  - IN CS-1 OBCSM 333
  - IN CS-1 TBCSM 334
  - AIN Toll-Free Service Example 334

IN CS-2/AIN 0.2 336
Originating Basic Call State Model (BCSM) 337
IN CS-2 OBCSM PICs 338
IN CS-2 OBCSM TDPs and Trigger Types 339
Terminating Basic Call State Model 342
IN CS-2 TBCSM PICs 342
IN CS-2 TBCSM TDPs and Trigger Types 343
AIN 0.2 Call Control Messages from the SCP 345
AIN 0.2 Time Of Day (TOD) Routing Example 346

Additional IN Service Examples 347
Local Number Portability (LNP) 347
Private Virtual Network (PVN) 350

Intelligent Network Application Protocol (INAP) 351
Basic Toll-Free Example Using INAP 354
Service Creation Environment (SCE) 355
Service Independent Building Blocks (SIB) 356
Service Logic Programs (SLP) 357

Summary 358

Chapter 12 Cellular Networks 361

Network Architecture 363
Mobile Station (MS) 366
IMEI 366
IMSI 367
TMSI 368
MSISDN 369
MSRN 369
Subscriber Identity Module (SIM) 369
Base Transceiver Station (BTS) 370
Base Station Controller (BSC) 370
Mobile Switching Centre (MSC) 370
Home Location Register (HLR) 370
Visitor Location Register (VLR) 371
Equipment Identity Register (EIR) 371
Authentication Center (AuC) 371
Serving GPRS Support Node (SGSN) 372
Gateway GPRS Support Node (GGSN) 372

Interfaces and Protocols 372
BSSAP (DTAP/BSSMAP) 375
Mobile Application Part (MAP) 376

Mobility Management and Call Processing 378
Location Update 378
Mobile Terminated Call (MTC) 379

Summary 381

Chapter 13 GSM and ANSI-41 Mobile Application Part (MAP) 383

MAP Operations 384

Mobility Management 384
Location Management 385
updateLocation 385
cancelLocation 386
sendIdentification 386
purgeMS 387
Handover 387
prepareHandover 387
sendEndSignal 387
processAccessSignaling 388
forwardAccessSignaling 388
prepareSubsequentHandover 389
Authentication Management 389
IMEI Management 389
Subscriber Management 390
insertSubscriberData 390
deleteSubscriberData 390
Fault Recovery 390
reset 391
forwardCheckSsIndication 391
restoreData 391

Operation and Maintenance 391
Subscriber Tracing 391
activateTraceMode 391
deactivateTraceMode 392
Miscellaneous 392

Call Handling 393
sendRoutingInfo (SRI) 394
provideRoamingNumber (PRN) 395

Supplementary Services 395
Unstructured Supplementary Services (USSs) 395
Operations 396

Short Message Service (SMS) 397
forwardSM 398
sendRoutingInfoForSM 398
reportSMDeliveryStatus 399
informServiceCentre 400

Summary 400

Part IV SS7/C7 Over IP 403

Chapter 14 SS7 in the Converged World 405

Next Generation Architecture 405

SigTran 407
Stream Control Transmission Protocol (SCTP) 409
Head-of-Line Blocking 410
Failure Detection 411
Multihoming and Failure Recovery 412
Proposed Additions 413

User Adaptation (UA) Layers 413
UA Common Terminology 414
Routing Keys and Interface Identifiers 416

MTP Level 3 UA (M3UA) 418
Messages and Formats 420
Transfer Messages 423
SS7 Signaling Network Management (SSNM) Messages 423
ASPSM and ASPTM Messages 425
Management (MGMT) Messages 426
Routing Key Management (RKM) Messages 427
SS7/C7 Variant Specifics 427
Message Flow Example 427

SCCP User Adaptation (SUA) 428
Messages and Formats 430
Connectionless Messages 432
Connection-Oriented Messages 432
MGMT Messages 433
ASPSM and ASPTM Messages 433
RKM Messages 433
Message Flow Example 434

MTP Level 2 User Adaptation (M2UA) 434
Messages and Formats 435
MTP2 User Adaptation (MAUP) Messages 437
SS7 Variant Specifics 439
Message Flow Examples 439
MTP Level 2 Peer Adaptation (M2PA) 440
M2PA and M2UA Comparison 441
M2PA Differences from Other UAs 442
Messages and Formats 442
Message Flow Example 443

ISDN User Adaptation (IUA) 444

Transport Adaptation Layer Interface (TALI) 445

Early Cisco SS7/IP Solution 445

SS7 and SIP/H.323 Interworking 448

Summary 451

Part V Supplementary Topics 453

Chapter 15 SS7 Security and Monitoring 455

Traffic Screening 455
Screening Considerations 457
MTP 457
SCCP 457

MTP3: Management Messages 458
Originating Point Code 459
Destination Point Code 459

SCCP 459
SCCP User Messages 460
Management Messages 460
Subsystem Prohibited (SSP) 460
Subsystem Allowed (SSA) 460
Subsystem Status Test (SST) 460

Parameters 461

Traffic Monitoring 461
Q.752 Monitoring Measurements 463
MTP: Link Failures 463
MTP: Surveillance 464
MTP: Detection of Routing and Distribution Table Errors 465

MTP: Detection of Increases in Link SU Error Rates 465
MTP: Detection of Marginal Link Faults 465
MTP: Link, Linkset, Signaling Point, and Route Set Utilization 466
MTP: Component Reliability and Maintainability Studies 467
SCCP: Routing Failures 468
SCCP: Configuration Management 469
SCCP: Utilization Performance 469
SCCP: Quality of Service 470
ISUP: Availability/Unavailability 471
ISUP: Errors 471
ISUP: Performance 472
TCAP Fault Management 472
TCAP Performance 472

Summary 473

Chapter 16 SS7 Testing 475

Test Equipment 476

Test Specification Creation 478

MTP 2 Testing 480
Test Configuration 480
Example 1: Initialization (Power-up), Test 1.1 481
Part (a) 481
Part (b) 482
Example 2: Normal Alignment—Correct Procedure (FISU), Test 1.5 482
Part (a) 483
Part (b) 483
Example 3: Individual End Sets Emergency, Test 1.22 484
Example 4: SIO Received During Link In-Service, Test 1.28 485
Example 5: Unexpected Signal Units/Orders in "In-Service" State, Test 2.7 485
Example 6: Link Aligned Ready (Break Tx Path), Test 3.1 486
Example 7: Link Aligned Ready (Corrupt FIBs—Basic), Test 3.2 487
Example 8: Set and Clear LPO While Link In-Service, Test 4.1 488
Example 9: SU Delimitation, Alignment, Error Detection, and Correction, Test 5.1 489
Example 10: Error Rate of 1 in 256—Link Remains In-Service, Test 6.1 490
Example 11, Test 7.1 491
Example 12: Check RTB Full, Test 8.3 492
Example 13: Forced Retransmission with the Value N1, Test 9.3 493
Example 14: Congestion Abatement, Test 10.1 495

MTP 3 Testing 496
Test Configuration 496
Example 1: First Signaling Link Activation, Test 1.1 497
Example 2: Load Sharing within a Linkset (All Links Available), Test 2.4.1 498
Example 3: Inaccessible Destination—Due to a Linkset Failure, Test 2.6.1 499

ISUP Testing 500
Test Configuration 502
Example 1: CCR Received—Successful, Test 1.4.1 502
Example 2: Overlap Operation (with SAM), Test 2.2.2 503
Example 3: Timers T1 and T5—Failure to Receive a RLC, Test 5.2.3 503

ISUP Supplementary Services Testing 504
Test Configuration 505
Example 1: CUG Call with Outgoing Access Allowed and Sent, Test 2.1.1 505
Example 2: CLIP—Network Provided and Sent, Test 3.1.1 506
Example 2: COL—Requested and Sent, Test 6.1.1 507

SCCP Testing 507
Test Configuration 508
Example 1: Local DPC and SSN Included, DPC and SSN Available, GT and SSN Included and Sent, Test 1.1.1.1.1.1 508
Example 2: Remote DPC and SSN Included, DPC and/or SSN Unavailable—Return Option Not Set, Test 1.1.1.1.6 509
Example 3: Local DPC and SSN, and SSN Available GT Not Included, SSN Included, Test 1.1.2.2.1.2 510

TCAP Testing 510
Test Configuration 512
Example 1: Clearing Before Subsequent Message; Valid Clearing from Initiating Side; Prearranged Ending, Test 1.1.2.1.1 (1) 512
Example 2: First Continue Message; OTID Absent, Test 1.2.2.3 (1) 513
Example 3: Inopportune Reject Component, Test 2.3.2.4 (1) 514

Summary 514

Part VI Appendixes 517

Appendix A MTP Messages (ANSI/ETSI/ITU) 519

Appendix B ISUP Messages (ANSI/UK/ETSI/ITU-T) 525

Appendix C SCCP Messages (ANSI/ETSI/ITU-T) 533

Appendix D TCAP Messages and Components 539

Appendix E ITU-T Q.931 Messages 543

Appendix F GSM and ANSI MAP Operations 549

Appendix G MTP Timers in ITU-T/ETSI/ANSI Applications 557

Appendix H ISUP Timers for ANSI/ETSI/ITU-T Applications 563

Appendix I GSM Mobile Country Codes (MCC) and Mobile Network Codes (MNC) 573

Appendix J ITU and ANSI Protocol Comparison 595

Appendix K SS7 Standards 599

Appendix L Tektronix Supporting Traffic 607

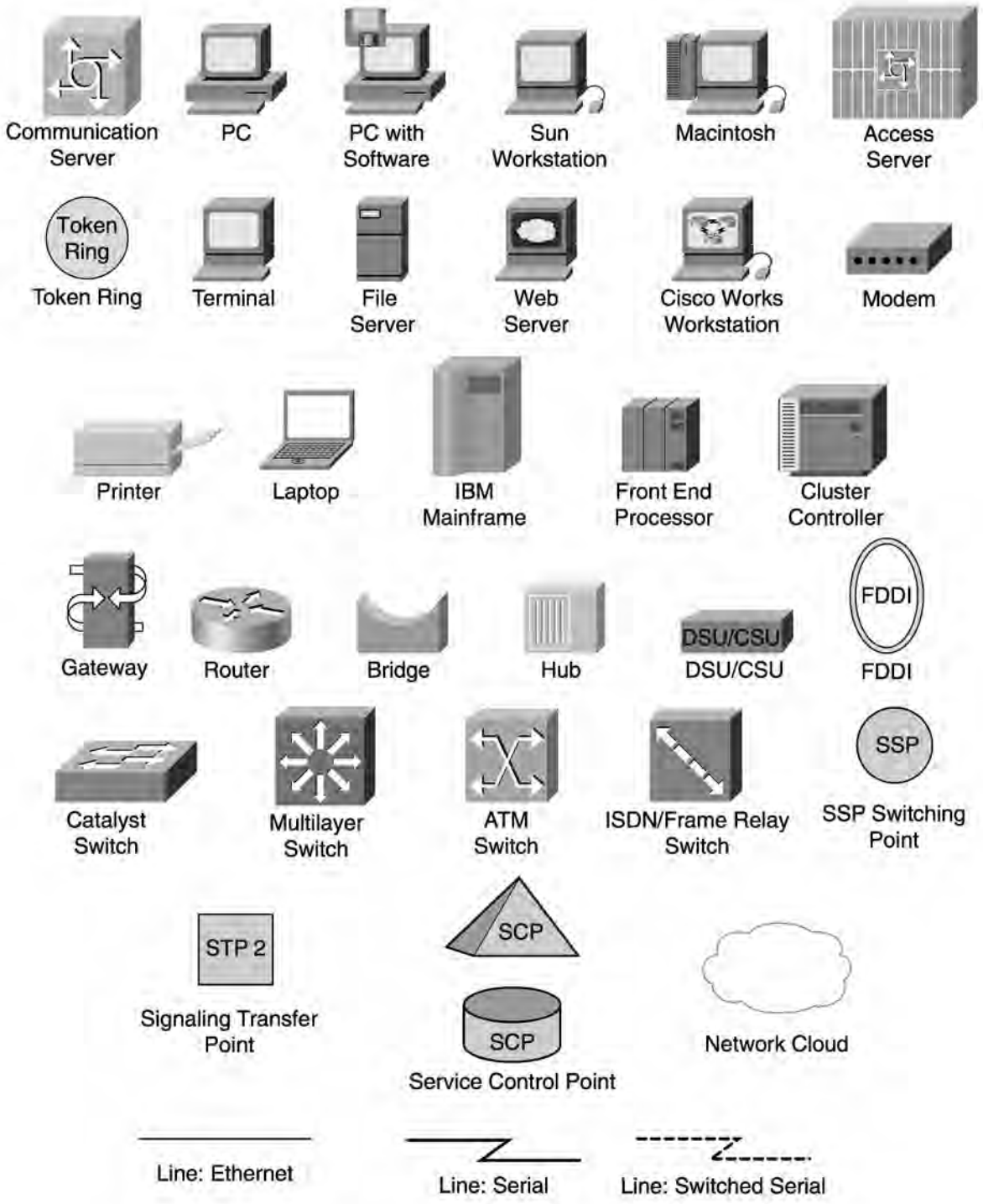
Appendix M Cause Values 637

Acronyms 643

References 665

Index 675

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same as the conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.
- **Bold** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), bold indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.

Reference Information

The chapters in this book include references to a variety of supporting documents, such as ITU-T and ANSI standards. These supporting documents are listed in the "References" section at the end of the book. Each document in this section is numbered. The corresponding number appears in the chapter text.

Introduction

SS7/C7 is a signaling network and protocol that is used worldwide to bring telecommunications networks, both fixed-line and cellular, to life. Setting up phone calls, providing cellular roaming and messaging, and converged voice/data services, such as Internet Call Waiting, are only a few of the vast number of ways that SS7/C7 is used in the communications network. SS7/C7 is at the very heart of telecommunications, and as voice networks and data networks converge, SS7/C7 will provide the technology to bridge the gap between the two worlds. Anyone who is interested in telecommunications should have a solid understanding of SS7/C7. The convergence of voice and data has extended the need to understand this technology into the realm of those working with data networks.

Who Should Read This Book?

This book was written in such a way that those who have a general interest in communications and those who are heavily involved in SS7/C7 can benefit. Although many of the earlier chapters are interesting to those who require only introductory knowledge, many of the later chapters are more interesting to those who have a deeper interest and are already involved in telecommunications.

How This Book Is Organized

Those who are new to the world of telecommunications signaling should read Chapters 1 to 5 first, in sequence. Those who are already comfortable with telecommunications and signaling concepts can read particular chapters of interest. This book should prove the most valuable for those who already consider themselves experts in SS7/C7; in particular, attention should be given to the extensive appendixes.

Part I: Introductions and Overviews

Chapter 1: The Evolution of Signaling

This chapter introduces the concept of signaling. It is a great starting point for those who are unfamiliar with signaling or telecommunications in general. It introduces concepts and terminology that are used throughout the book.

Chapter 2: Standards

This chapter introduces the relevant standards and the bodies that are involved in creating them. It also provides some background on both the history of the standards and the bodies themselves. In addition, it introduces the concept of standards on different planes—national, regional, and international.

Chapter 3: The Role of SS7

This chapter is an excellent introduction to SS7/C7 and its relevance. Any reader can read it, regardless of background. Hopefully even those who are very knowledgeable in SS7/C7 will find this chapter interesting, because it lists the functions and services offered by SS7/C7 and explains its relevance in the daily lives of people across the globe.

Chapter 4: SS7 Network Architecture and Protocols Introduction

This chapter provides a technical overview of the SS7 protocol and network architecture. Those who are new to the subject will find it particularly interesting. It provides an introductory technical overview of SS7 in such a way that newcomers can assimilate subsequent chapters more effectively.

Chapter 5: The Public Switched Telephone Network (PSTN)

This chapter provides a brief overview of the Public Switched Telephone Network. It helps you understand SS7 in its native environment as the primary form of interoffice signaling in the PSTN. It also briefly introduces the PSTN's transition to the next-generation Voice Over Packet architecture.

Part II: Protocols Found in the Traditional SS7/C7 Stack

Chapter 6: Message Transfer Part 2 (MTP2)

This chapter examines the first protocol on top of the physical layer. It covers frame format, functions, and procedures—packet delineation, error correction, error detection, alignment, managing the signaling link, procedures for establishing a signaling link, flow control, and link error monitoring.

Chapter 7: Message Transfer Part 3 (MTP3)

This chapter covers the core concepts of how SS7 network nodes communicate with each other. It discusses network addressing and routing in detail, along with examples of how messages flow through an SS7 node. It also explains the numerous messages and procedures that MTP3 uses to maintain a healthy network.

Chapter 8: ISDN User Part (ISUP)

This chapter explains how the ISUP portion of the protocol is used to set up and tear down calls, provide trunk maintenance functions, and deliver supplementary services. It defines ISUP message structure as well as the most commonly used messages and parameters. The association between call processing at an SSP and the ISUP protocol is described, thereby helping you understand how an SS7-signaled call is processed at an SSP.

Chapter 9: Signaling Connection Control Part (SCCP)

This chapter looks at the enhanced functionality that the addition of this protocol brings—namely, application management, more flexible and powerful routing through the use of global titles, and mechanisms for transferring application data over the signaling network.

Chapter 10: Transaction Capabilities Application Part (TCAP)

This chapter describes the role of TCAP in providing a generic protocol mechanism for transferring information components between applications across the network. It helps you understand the key role TCAP plays in communication between SSP and SCP nodes. TCAP message formats and component definitions, including ITU and ANSI formats, are explained.

Part III: Service-Oriented Protocols

Chapter 11: Intelligent Networks (IN)

This chapter explains the concept of the Intelligent Network, how it has evolved, and how it is used to implement telecommunications services. It provides a detailed explanation of the IN call model and explains the parallels and differences between the ITU CS model and the North American AIN model. Several examples of IN services, such as toll-free calling and local number portability, are included to show how IN services are used.

Chapter 12: Cellular Networks

This chapter introduces GSM public land mobile networks (PLMNs) so that the following chapter can cover additional SS7 protocols used in cellular networks. It introduces cellular network entities, addressing, terminology, and concepts.

Chapter 13: GSM and ANSI-41 Mobile Application Part (MAP)

This chapter explains the operations and associated procedures that allow cellular subscribers to have mobility; this is the key functionality expected of a cellular network. Subscriber authentication, operations and maintenance, supplementary service, unstructured supplementary service (USS), and short message service (SMS) operations and procedures are also detailed.

Part IV: SS7/C7 Over IP

Chapter 14: SS7 in the Converged World

This chapter introduces the next-generation network architecture using media gateway controllers, media gateways, and signaling gateways. Its primary purpose is to provide an in-depth look at the Signaling Transport protocol (Sigtran), used between the media gateway controller and the signaling gateway. Sigtran is particularly interesting to those who are learning about SS7, because it provides a common signaling protocol interface between legacy SS7 networks and voice over IP networks.

Part V: Supplementary Topics

Chapter 15: SS7 Security and Monitoring

This chapter explains the need for SS7/C7 security practices. It describes the current means of providing security: traffic screening and monitoring. Details of providing traffic screening are supplied. Monitoring functionality and what should be monitored also are covered.

Chapter 16: SS7 Testing

This chapter explains the tools used for SS7/C7 protocol verification and how to create appropriate test specifications. It also outlines sample test cases for each protocol layer.

Part VI: Appendixes

Appendix A: MTP Messages (ANSI/ETSI/ITU)

This appendix lists all of the messages used by MTP3 for ANSI- and ITU-based networks. It also lists the message codes.

Appendix B: ISUP Messages (ANSI/UK/ETSI/ITU-T)

This appendix lists all of the messages used by ISUP for ANSI- and ITU-based networks. It also lists the message codes.

Appendix C: SCCP Messages (ANSI/ETSI/ITU-T)

This appendix lists all of the messages used by SCCP for ANSI- and ITU-based networks. It also lists the message codes.

Appendix D: TCAP Messages and Components

This appendix lists all of the messages and components used by MTP3 for ANSI- and ITU-based networks. It also lists the message codes.

Appendix E: ITU-T Q.931 Messages

Q.931 is the Layer 3 protocol of the subscriber signaling system that is used for ISDN, known as Digital Subscriber Signaling System No. 1 (DSS 1). It employs a message set that is made for interworking with SS7's ISUP. This appendix lists and describes the purpose of the Q.931 message set.

Appendix F: GSM and ANSI MAP Operations

This appendix lists the operations found in GSM MAP and their respective codes.

Appendix G: MTP Timers in ITU-T/ETSI/ANSI Applications

This appendix lists ANSI- and ITU-specified MTP timers.

Appendix H: ISUP Timers for ANSI/ETSI/ITU-T Applications

This appendix lists ANSI- and ITU-specified ISUP timers.

Appendix I: GSM Mobile Country Codes (MCC) and Mobile Network Codes (MNC)

This appendix lists all of the MCC codes and the respective MNCs found against the MCC.

Appendix J: ITU and ANSI Protocol Comparison

This appendix covers some of the main differences between ANSI and ITU (international).

Appendix K: SS7 Standards

This appendix presents the main SS7 standards alongside the respective standards body.

Appendix L: Tektronix Supporting Traffic

This appendix contains reference traffic caught on a Tektronix K1297 protocol analyzer.

Appendix M: Cause Values

Cause values, which are included as a field in each ISUP REL message, indicate why a call was released. This appendix lists and defines the ITU-T and ANSI cause values.

CHAPTER 1

The Evolution of Signaling

This chapter is intended to provide a sound introduction to the world of telecommunications signaling. It is particularly written for those readers who have little or no signaling knowledge. It provides a solid foundation to help you grasp signaling ideas, concepts, terminology, and methods. A strong foundation will provide the novice reader with a better understanding of the book's main topic: Signaling System No. 7. Today, Signaling System No. 7 is the most advanced and widely used signaling system for both cellular and fixed-line telecommunications networks.

This chapter covers the following topics:

- What signaling is and why it is relevant
- Overview of subscriber and network signaling
- The history of signaling and the development of the Public Switched Telephone Network (PSTN)
- Overview of the Channel Associated Signaling (CAS) method of signaling and its common implementations
- Overview of the Common Channel Signaling (CCS) method of signaling and its operational modes
- The limitations of CAS and CCS

Signaling System No. 7, known more commonly in North America as SS7 and elsewhere as C7, is both a network architecture and a series of protocols that provide telecommunications signaling. In order to begin studying SS7, you must first learn what telecommunications signaling is by studying its origins and purpose.

The ITU-T defines signaling as, [47] "The exchange of information (other than by speech) specifically concerned with the establishment, release and other control of calls, and network management, in automatic telecommunications operation."

In telecommunications, the network's components must indicate (that is, signal) certain information to each other to coordinate themselves for providing services. As such, the signaling network can be considered the telecommunications network's nervous system. It breathes life into the infrastructure. Richard Manterfield, author of *Telecommunications Signaling*, has stated this poetically [103]:

"Without signaling, networks would be inert and passive aggregates of components. Signaling is the bond that provides dynamism and animation, transforming inert components into a living, cohesive and powerful medium."

For example, if a subscriber wishes to place a call, the call must be signaled to the subscriber's local switch. The initial signal in this process is the off-hook condition the subscriber causes by lifting the handset. The action of lifting the handset signals to the network that the subscriber wishes to engage telephony services. The local switch should then acknowledge the request for telephony services by sending back a dial tone, which informs the subscriber that he can proceed to dial the called party number. The subscriber has a certain amount of time to respond to the dial tone by using the telephone keypad to signal the digits that comprise the called party number. The network signals that it is receiving the dialed digits with silence (as opposed to a dial tone).

Up to this point, the signaling is known as *subscriber signaling* and takes place between the subscriber and the local switch. Subscriber signaling is also known as *access signaling*. The "Subscriber Signaling" section of this chapter further describes subscriber signaling.

NOTE The calling party is often referred to as the A party. Similarly, the called party is referred to as the B party.

When a complete called party number is received or enough digits are collected to allow the routing process to proceed, the calling party's local switch begins signaling to the other nodes that form part of the core network.

The signaling that takes place between core network nodes (and switches and, over the past two decades, databases) is known as network signaling.

NOTE Switches are also known as exchanges; within the United States, the term exchange is used interchangeably with Central Office (CO) or End Office (EO).

Network signaling is also known as inter-switch signaling, network-network signaling, or trunk signaling.

The purpose of network signaling is to set up a circuit between the calling and called parties so that user traffic (voice, fax, and analog dial-up modem, for example) can be transported

bi-directionally. When a circuit is reserved between both parties, the destination local switch places a ringing signal to alert the called party about the incoming call. This signal is classified as subscriber signaling because it travels between a switch (the called party's local switch) and a subscriber (the called party). A ringing indication tone is sent to the calling party telephone to signal that the telephone is ringing. If the called party wishes to engage the call, the subscriber lifts the handset into the off-hook condition. This moves the call from the set-up phase to the call phase.

At some point in the call phase, one of the parties will wish to terminate the call, thereby ending the call phase. The calling party typically initiates this final phase, which is known as the clear-down or release phase. The subscriber signals the network of the wish to terminate a call by placing the telephone back in the on-hook condition; hence, subscriber signaling. The local switch proceeds with network signaling to clear the call down. This places an expensive resource (the circuit) back to an idle condition, where it can be reserved for another call.

The previous high-level example relates to a basic telephone service call; that is, simple call setup and clear down. As you will discover, the signaling network can do far more than carry the digits you dial, release calls, notify the network that you went on or off-hook, and so forth. The signaling network can also translate toll-free numbers into "routable" numbers, validate credit and calling cards, provide billing information, remove faulty trunks from service, provide the support for supplementary services (such as caller ID), allow you to roam with your cellular telephone, and makes *local number portability (LNP)* possible. This list is by no means exhaustive; see Chapters 3, "The Role of SS7," and 11, "Intelligent Networks (IN)," for more example services.

The main function of signaling is still that of circuit supervision: setting up and clearing down circuits (that is, trunks). Traditionally, once a circuit was set up, no other signaling was performed apart from releasing the call; therefore, all calls were simple, basic telephone service calls. However, modern telephone networks can perform signaling while a call is in progress, especially for supplementary services—for example, to introduce another called party into the call, or to signal the arrival of another incoming call (call waiting) to one of the parties. In fact, since the 1980s, signaling can take place even when there is not a call in place. This is known as *non-circuit related signaling* and is simply used to transfer data between networks nodes. It is primarily used for query and response with telecommunications databases to support cellular networks, intelligent networks, and supplementary services. For example, in Public Land Mobile Networks (PLMNs), the visitor location register (VLR) that is in charge of the area into which the subscriber has roamed updates the home location register (HLR) of the subscriber's location. PLMNs make much use of non-circuit-related signaling, particularly to keep track of roaming subscribers. Chapter 13, "GSM and ANSI-41 Mobile Application Part (MAP)," covers this topic in more detail.

Network signaling is further described in the "Network Signaling" section of this chapter.

The History of Signaling

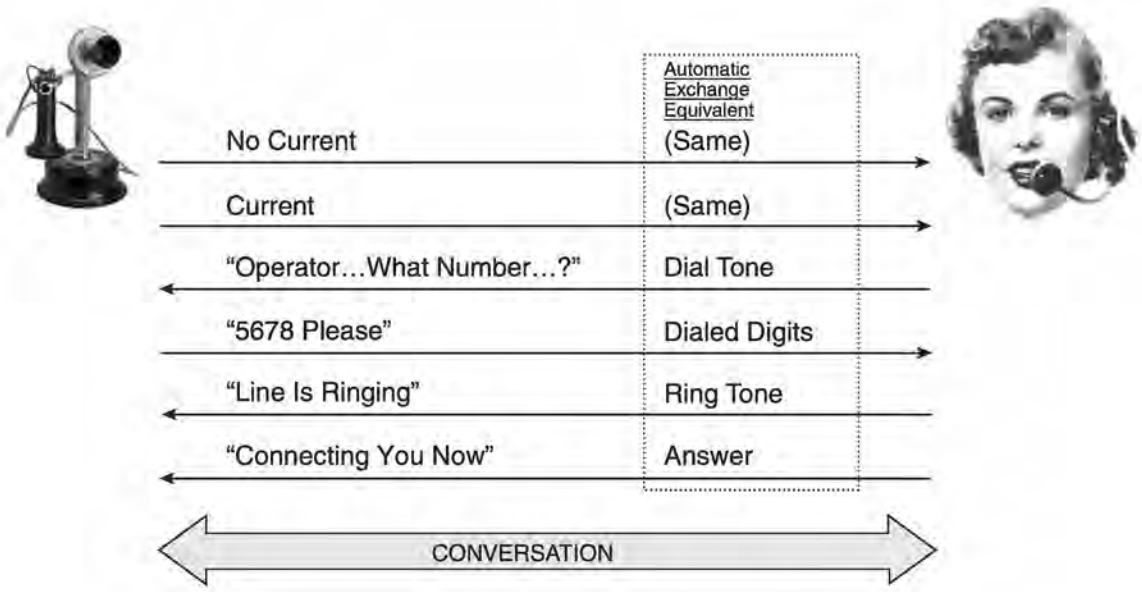
To appreciate signaling in today's network and its role in future networks, let's examine the history of signaling. The history of signaling has been inextricably linked to the history of telecommunications and, in particular, switching. As telecommunications advances, so do the signaling systems that support it.

1889–1976

The earliest telephone switches were manual; operators used a switchboard and wire cords to connect and disconnect all calls. The first manual exchange occurred in 1878 in New Haven, Connecticut. It was introduced to avoid the imminent problem of running wires from each telephone to every other telephone (a fully meshed topology). The first manual switch appeared in Great Britain in 1879. It was also within this same year that subscribers came to be called by numbers rather than by names. Within a decade of introducing the manual switch, the United States had 140,000 subscribers and a staggering 8000 exchanges—that is, a switch for every 17.5 subscribers!

A subscriber who was connected to a manual switch would crank a lever to electronically send an alerting signal that lit up a bulb on the operator's switchboard. The operator would then connect her telephone to the calling line, and ask for the called number. Next the operator would connect her telephone to the called line, where she would place a ringing signal. If the called party answered the call, the operator would establish the connection by plugging in a cord between the two terminal jacks on the switchboard. Figure 1-1 shows this process; on the switchboard, each terminal jack represents a subscriber.

Figure 1-1 *Simple Call Setup Via a Manual Operator with Automatic Equivalent*



Signaling, as we know it today, began around 1889 with the invention of the Strowger exchange (which was patented 1891). The Strowger exchange was an electromechanical device that provided automatic switching using the simple idea of two-motion selectors for establishing calls between two subscribers. It was also known as a step-by-step switch because it followed pre-wired switching stages from start to finish.

Inventing the Strowger Exchange

Almon B. Strowger was a schoolteacher and part-time undertaker. His reportedly constant feuds with manual switchboard operators inspired him to develop an automatic switching system and the dial telephone so he could bypass manual switchboard operators [102]. One reported feud concerned an alleged business loss resulting from the complete lack of privacy offered by a manual exchange. Strowger claimed that an operator at the new manual exchange in Connecticut had intentionally directed a call to a competitor—an allegation that gave rise to tales that the operator was either married to or was the daughter of a competing undertaker. Strowger moved from Topeka to Kansas City, where he hoped his new, larger funeral home would earn him his fortune. However, he suffered a similar fate there; he believed that the manual operators there were intentionally giving his customers a busy signal. Strowger therefore decided to do away with operators; he hired several electromechanical technicians, who created the first automatic exchange within a year. As a result, the telephone became faster, easier to use, and more private for everyone.

The first Strowger exchange in the United States opened in La Porte, Indiana in 1892 and had the switching capacity for ninety-nine lines. Lobby groups protested at the automatic exchange, and one lobby group championed the personalized service afforded by manual exchanges. The lobby group did not have much success, however; manual switchboards could not service the dramatic increase in telephone subscribers. By 1900 there were 1.4 million telephones in the United States.

In Great Britain, the first Strowger exchange opened at Epsom in Surrey in 1912. The last Strowger switch was not removed from the British Telecom (BT) service network until June 23, 1995, when it was removed from Crawford, Scotland.

Strowger sold his patents to his associates for $1,800 in 1896 and sold his share in the company for $10,000 in 1898. He died in 1902. In 1916, his patents were sold to Bell Systems for $2.5 million dollars.

Strowgers' dial telephone is considered the precursor of today's touch-tone phone. It had three buttons: one for hundreds, one for tens, and one for units. To call the number 322, the caller had to push the hundreds button three times, the tens button two times, and the units button two times.

In 1896 the Automatic Electric Company developed a rotary dial to generate the pulses. This method of transmitting the dialed digits became known as *pulse dialing* and was

commonplace until the latter half of the twentieth century, when *tone dialing* became available. See "Address Signals" in the "Subscriber Signaling" section of this chapter for a discussion of pulse and touch-tone dialing. It is interesting to note that early users did not like the dial pulse handset because they felt they were doing the "telephone company's job."

Even in Great Britain in 1930, the majority of all local and long distance calls were still connected manually through an operator. But gradually, calls placed between subscribers served by the same local switch could be dialed without the help of an operator. Therefore, only subscriber signaling was required because an operator would perform any inter-switch signaling manually. In the decades that followed, it became possible to dial calls between subscribers who were served by nearby switches. Thus the requirement for network signaling was born. Most large U.S. cities had automatic exchanges by 1940.

Direct Distance Dialing (*DDD*) was introduced in the United States in the 1950s. DDD allowed national long distance calls to be placed without operator assistance, meaning that any switch in the United States could route signaling to any other switch in the country. *International Direct Distance Dialing* (IDDD) became possible in the 1960s, thus creating the requirement for signaling between international switches.

From 1889 to 1976, signaling had three main characteristics, which resulted because only basic telephone services were available [102]:

- Signaling was fairly simple. All that was required of the signaling system was the setting-up and releasing of circuits between two subscribers.
- Signaling was always circuit-related; that is, all signals related directly to the setting-up or clearing of circuits.
- There was a deterministic relationship, known as *Channel Associated Signaling (CAS)*, between the signaling and the voice traffic it controlled. The "Channel Associated Signaling" section of this chapter discusses CAS.

1976 to Present Day

Another form of signaling was introduced in 1976: *Common Channel Signaling* (CCS). The "Common Channel Signaling" section of this chapter further explains CSS.

CCS has been used to implement applications beyond the scope of basic telephone service, including Intelligent Networks (INs), supplementary services, and signaling in cellular mobile networks. As you will learn, SS7 is the modern day CCS system that is used for network signaling. As with any technical subject, signaling can be split into a number of classifications. The broadest classification is whether the signaling is subscriber or networked signaling. The following sections discuss these types of signaling.

Subscriber Signaling

Subscriber signaling takes place on the line between the subscribers and their local switch. Most subscribers are connected to their local switch by analog subscriber lines as opposed to a digital connection provided by an Integrated Services Digital Network (ISDN). As a result, subscriber signaling has evolved less rapidly than network signaling.

Subscriber signals can be broken down into the following four categories:

- Address Signals
- Supervisory Signals
- Tones and Announcements
- Ringing

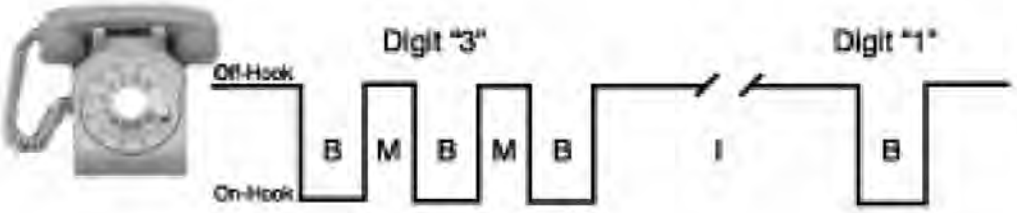
Address Signals

Address signals represent the called party number's dialed digits. Address signaling occurs when the telephone is off-hook. For analog lines, address signaling is either conveyed by the dial pulse or Dual-Tone Multiple Frequency (DTMF) methods. Local switches can typically handle both types of address signaling, but the vast majority of subscribers now use Dual-Tone Multi Frequency (DTMF), also known as touch-tone.

The precursor to (DTMF) was dial pulse, which is also known as rotary dialing. In rotary dialing, the address signals are generated by a dial that interrupts the steady DC current at a sequence determined by the selected digit. The dial is rotated clockwise, according to the digit selected by the user. A spring is wound as the dial is turned; when the dial is subsequently released, the spring causes the dial to rotate back to its original resting position. Inside the dial, a governor device ensures a constant rate of return rotation, and a shaft on the governor turns a cam that opens and closes switch contact. The current flowing into the telephone handset is stopped when the switch contact is open, thereby creating a dial pulse. As the dial rotates, it opens and closes an electrical circuit.

The number of breaks in the string represents the digits: one break for value 1, two breaks for value 2, and so on (except for the value of 0, which is signaled using ten breaks). The nominal value for a break is 60 ms. The breaks are spaced with make intervals of nominally 40 ms. As shown in Figure 1-2, consecutive digits are separated by an inter-digit interval of a value greater than 300 ms.

Figure 1-2 *Dial Pulse Address Signals*



The rotary dial was designed for operating an electromechanical switching system; the speed of the dial's operation was approximately to match the switches' operating speed.

DTMF is a modern improvement on pulse dialing that first appeared during the 1960s and is now widespread. A DTMF signal is created using a pair of tones, each with a different frequency. It is much faster than the previous pulse method and can be used for signaling after call completion (for example, to operate electronic menu systems or activate supplementary services, such as a three-way call). The standard DTMF has two more buttons than dial pulse systems: the star (*) and the pound, or hash (#) buttons. These buttons are typically used in data services and customer-controlled features. The CCITT has standardized the DTMF frequency combinations, as shown in Table 1-1. For additional information regarding the CCITT, see Chapter 2, "Standards."

Table 1-1 *Tones Used to Create DTMF Signals*

	1209 Hz	**1336 Hz**	**1477 Hz**	**1633 Hz**
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

The fourth column (1633 Hz) has several special uses that are not found on regular telephones. The four extra digits were used on special handsets to designate the priority of calls on the Automatic Voice Network (AUTOVON), the U.S. military phone network that has since been replaced with the Defense Switched Network (DSN). In AUTOVON, the keys were called Flash, Immediate, Priority, and Routine (with variations) instead of ABCD. Telephone companies still use the extra keys on test handsets for specific testing purposes.

All modern telephone handsets support both DTMF and dial pulse. Because an electronic handset has buttons rather than a rotary dial, the numbers are temporally stored in the telephone memory to generate pulse dialing. The handset then transmits the dial pulses. This arrangement is sometimes known as *digipulse*.

Supervisory Signals

A telephone has two possible supervision states: *on-hook* or *off-hook*. On-hook is the condition in which the telephone is not in use, which is signaled when the telephone handset depresses the cradle switch. The term on-hook comes from the days when the receiver part of the telephone rested on a hook. The telephone enters the off-hook condition when the handset is lifted from its cradle, thereby releasing the cradle switch and signaling to the exchange that the subscriber wishes to place an outgoing call.

Residential systems worldwide use a change in electrical conditions, known as *loop start signaling*, to indicate supervision signals. The local switch provides a nominal –48 V direct current (DC) battery, which has the potential to flow through the subscriber line (between the local switch and the subscriber). When a telephone is off-hook, DC can flow in the subscriber line; when a telephone is on-hook a capacitor blocks the DC. The presence or absence of direct current in the subscriber's local switch line determines the telephone's supervision state. Loop start systems are adequate for residential use, but a problem known as *glare* makes loop start unacceptable in typical business applications in which private exchanges (PBXs) are used. PBXs use a system known as *ground start signaling*, particularly in North America.

Ground start systems combat glare by allowing the network to indicate off-hook (seizure) for incoming calls, regardless of the ringing signal. This reduces the probability of simultaneous seizure, or glare, from both ends. Ground start requires both ground and current detectors in customer premise equipment (CPE).

Tones and Announcements

Tones and announcements are audible backward signals, such as dial tone, ring back, and busy-tone, that are sent by a switch to the calling party to indicate a call's progress. Table 1-2 shows the call progress tones that are used in North America.

Table 1-2 *Call Progress Tones Used in North America*

Tone	Frequency (Hz)	On Time (Sec)	Off Time (Sec)
Dial	350+440	Continuous	
Busy	480+620	0.5	0.5
Ring back, Normal	440+480	2	4
Ring back, PBX	440+488	1	3
Congestion (Local)	480+620	0.3	0.2
Congestion (Toll)	480+620	0.2	0.3
Howler (Receiver wrongly off-hook)	1400+2060+2450+2600	0.1	0.1

Forward signals refer to signals that transfer in the direction of call establishment, or from the calling party to the called party. Backward signals refer to signals that transfer in the reverse direction.

Ringing

Ringing is a forward signal sent by the switch to the called subscriber to indicate the arrival of a call. It is known more specifically as power ringing to distinguish it from audible ringing, which is played to the calling party to alert him that the called party phone is ringing. Each country has a ringing pattern, which is known as the *cadence*. In North America the pattern is two seconds on, four seconds off.

Note that audible and power ringing are not synchronized. This is why, on a rare occasion, a caller is already on the line when you lift the handset. This situation generally causes confusion because the calling party, who has heard audible ringing, is unaware of the problem since the problem occurs because the caller's switch does not generate an independent ringing signal for each line. Instead, it generates one signal that is applied to whichever lines are to be played audible ringing. Therefore, if you have an incoming call, the switch must wait until the next on-cycle to ring your telephone. If you happen to pick up the telephone during the few off-cycle seconds and a call has just come in, you have answered a call before the exchange has had the opportunity to alert you of the incoming call. In North America, the silent period during which inbound calls cannot be announced is 3.9 seconds. Countries that use a short period of silence in the ringing cadence are less susceptible to this problem.

NOTE If you are one of those people who say that you will call home and let the telephone ring twice when you get to your destination safely, note that you have no guarantee that the telephone will actually ring twice—or even ring at all. You might hear two rings, but that does not mean the called party will hear two, or even any, rings because their power ringing pattern might be in an off period.

The problems associated with the lack of synchronization between the calling and called party is typically addressed in North American non-residential systems (PBX systems) by using ground start rather than loop start. Other countries often employ a simple technique known as *ring splash*. With ring splash, a PBX issues a brief ringing tone within a few hundred milliseconds of the trunk being seized (the incoming call), after which normal ringing cadence resumes. The downside to this solution is that the ringing cadence sounds strange because it is not synchronized with the initial ring.