THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco BTS 10200 Softswitch Operations Manual
Copyright © 2004, Cisco Systems, Inc.
All rights reserved.
CONTENTS

Preface xxii
  Audience xxii
  Modification History xxii
  Document Organization xxiii
  Notes, Cautions, Warnings, and Tips xxiv
  Conventions xxv

Obtaining Documentation xxv
  World Wide Web xxv
  Documentation CD-ROM xxvi
  Ordering Documentation xxvii
  Documentation Feedback xxvii

Obtaining Technical Assistance xxviii
  Cisco.com xxviii
  Technical Assistance Center xxix
    Contacting TAC by Using the Cisco TAC Website xxix
    Contacting TAC by Telephone xxix

CHAPTER 1 Hardware 1
  Rack Configuration 1
  Powering On and Off 3
    Power On Procedure 3
    Power Off Procedure 4
  Hardware Monitoring 5
    CPU 5
    Memory Consumption 5
    Disk and Disk Utilization 5
    Alarm Reports 5
  Alarm Panel 6
  Disk Replacement 7
    Before You Start 7
  Replacing Disk 0 on CA/FS and EMS 7
  Replacing Disk 1 on CA/FS and EMS 11
  Deactivating and Activating Omni 14
CHAPTER 2 Operator Interfaces

Deactivating Omni 14
Activating Omni 15

Logging in Using Secure Shell 2
Bulk Provisioning 3
  Preparing a Script File on your Local System 3
  Connecting to the EMS 4
  Transferring a Script File to the EMS 4
  Confirming that a Script File Has Been Processed 5

EMS Services 5
  EMS Users and Services Commands 5
    Show 5
    Change 5
    EMS NTP Server Configuration 5

CHAPTER 3 Provisioning External Media Gateways

CHAPTER 4 Managing Access and Users

User and Command Privilege Levels 1
Command Level Provisioning 2
User Account Administration 2
  Users 2
    Show, Add, Change, Delete 3
    Invalid User Privilege Level 4
  User and Optiuser Set Password/Reset Password 4
  Command Table 5
  Workgroups 6
  Security Summary Report 6
  Session Manager 7
    Show Command 8
    Block Command 8
    Change Command 9
    Unblock Command 9
    Stop Command 9

CHAPTER 5 Provisioning the Call Agent, Subscribers, and Equal Access

Provisioning the Call Agent 1
Provisioning an Individual Subscriber 3
Provisioning Equal Access 4

CHAPTER 6
Provisioning Features and Services 1
800 Local Dialed Number Identification Service 2
Prerequisites 2
Supported Interfaces 2
Provisioning 800 Local DNIS 2
800 Local Time of Day and Day of Week 3
Prerequisites 3
Supported Interfaces 3
Provisioning 800 Local TOD and DOW 3
800 Policy Point of Presence Routing 4
Prerequisites 4
Supported Interfaces 4
Provisioning an 800 Policy POP 4
Anonymous Call Rejection 5
Prerequisites 5
Supported Interfaces 5
Provisioning ACR 5
Provisioning ACR for a Centrex Group 6
Automatic Callback 6
Prerequisites 6
Supported Interfaces 7
Provisioning AC 7
Provisioning AC for a Centrex Group 8
Automatic Number Identification Screening 8
Prerequisites 8
Supported Interfaces 8
Provisioning ANI Screening 9
Automatic Recall 10
Prerequisites 10
Supported Interfaces 10
Provisioning AR 10
Provisioning AR for a Centrex Group 11
Busy Line Verification and Busy Line Interrupt 11
Prerequisites 12
Supported Interfaces 12
Provisioning Office BLV 12
Provisioning BLV for Subscribers, Centrex, and M LHG 13

Call Admission Control Using the Resource Reservation Protocol 14
Prerequisites 14
Supported Interfaces 14
Provisioning Call Admission Control 14

Call Block 14
Prerequisites 14
Supported Interfaces 15
Provisioning Office Call Block 15
Provisioning Call Block for a Subscriber 15
Provisioning Call Block for Centrex Subscribers 15
Provisioning Call Block for M LHG Subscribers 16

Call Forwarding Busy 16
Prerequisites 16
Supported Interfaces 16
Provisioning CFB 16
Provisioning CFB for Centrex Subscribers 17

Call Forwarding No Answer 17
Prerequisites 17
Supported Interfaces 17
Provisioning CFNA 18
Provisioning CFNA for Centrex Subscribers 18

Call Forwarding Unconditional 19
Prerequisites 19
Supported Interfaces 19
Provisioning CFU 19
Provisioning CFU for Centrex Subscribers 20

Call Hold 20
Prerequisites 20
Supported Interfaces 20
Provisioning CHD 20

Call Park 21
Prerequisites 21
Supported Interfaces 21
Provisioning Call Park 21

Call Transfer 22
Prerequisites 22
Supported Interfaces 22
Provisioning CT 22
Call Waiting 23
Prerequisites 23
Supported Interfaces 23
Provisioning CW 23

Call Waiting Deluxe 24
Prerequisites 24
Supported Interfaces 24
Provisioning CWD 24
Provisioning CWD for Centrex Subscribers 25

Calling Identity Delivery and Suppression 25
Prerequisites 25
Supported Interfaces 25
Provisioning CIDS 25
Provisioning CIDS for Centrex Subscribers 26

Calling Identity Delivery on Call Waiting 26
Prerequisites 26
Supported Interfaces 26
Provisioning CIDCW 27
Provisioning CIDCW for Centrex Subscribers 27

Calling Name Delivery 27
Prerequisites 27
Supported Interfaces 28
Provisioning CNAM 28
Provisioning CNAM for Centrex Subscribers 28

Calling Number Delivery 29
Prerequisites 29
Supported Interfaces 29
Provisioning CND 29
Provisioning CND for Centrex Subscribers 29

Calling Name Delivery Blocking 30
Prerequisites 30
Supported Interfaces 30
Provisioning CNAB 30
Provisioning CNAB for Centrex Subscribers 31

Calling Number Delivery Blocking 31
Prerequisites 31
Supported Interfaces 31
Provisioning CNDB 31
Provisioning CNDB for Centrex Subscribers 32
Cancel Call Waiting  32
   Prerequisites  32
   Supported Interfaces  32
   Provisioning CCW  32
   Provisioning CCW for Centrex Subscribers  33
Centrex Direct Inward Dial and Direct Outward Dial  33
   Prerequisites  33
   Supported Interfaces  33
   Provisioning Centrex DID and DOD  33
Centrex Extension Dial  33
   Prerequisites  34
   Supported Interfaces  34
   Provisioning CED  34
Centrex POTS Access Code  36
   Prerequisites  36
   Supported Interfaces  36
   Provisioning Centrex PAC  36
Class of Service  36
   Prerequisites  36
   Supported Interfaces  37
   Provisioning Office COS  37
   Provisioning COS for Subscriber, Centrex and M LHG  38
Codec Negotiation  38
   Prerequisites  38
   Supported Interfaces  38
   Provisioning Codec Negotiation  39
Codec Selection  39
   Prerequisites  39
   Supported Interfaces  39
   Provisioning CS  39
Customer Originated Trace  40
   Prerequisites  40
   Supported Interfaces  40
   Provisioning a COT  40
   Provisioning Centrex COT  42
Direct Inward Dial Foreign Exchange Office  42
   Prerequisites  42
   Supported Interfaces  42
   Provisioning DID FXO  42
Directed Call Pickup With and Without Barge-in 43
  Prerequisites 43
  Supported Interfaces 44
  Provisioning DPN and DPU 44
    Provisioning DPN 44
    Provisioning DPU 44

Distinctive Alerting Call Waiting Indicator 45
  Prerequisites 45
  Supported Interfaces 45
  Provisioning a DACWI 45

Distinctive Ringing Call Waiting 45
  Prerequisites 45
  Supported Interfaces 46
  Provisioning DRCW 46
  Provisioning Centrex DRCW 46

Do Not Disturb 46
  Prerequisites 46
  Supported Interfaces 47
  Provisioning DND 47
  Provisioning Centrex DND 47

Dual Tone Multifrequency Relay 48
  Prerequisites 48
  Supported Interfaces 48
  Provisioning DTMF Relay 48

Hotline 48
  Prerequisites 48
  Supported Interfaces 48
  Provisioning Hotline 49
  Provisioning Hotline for Centrex 49

Local Number Portability 50
  Prerequisites 50
  Supported Interfaces 50
  Provisioning LNP 50

Multiline Hunt Group 51
  Prerequisites 51
  Supported Interfaces 51
  Provisioning a POTS MLHG 51
  Provisioning a Centrex MLHG 52

Multiple Directory Number 53
Prerequisites 53
Supported Interfaces 53
Provisioning an MDN 53

Network Access Server 54
Prerequisites 54
Supported Interfaces 54
Provisioning NAS 54

Operator Services 55
Prerequisites 55
Supported Interfaces 55
Provisioning Operator Services 56

Originating Line Information Screening 57
Prerequisites 57
Supported Interfaces 57
Provisioning OLI 57

Outgoing Call Barring 58
Prerequisites 58
Supported Interfaces 58
Provisioning OCB 58
Provisioning OCB 58
Provisioning OCB for Centrex 59

Remote Activation of Call Forwarding and Pin Change 60
Prerequisites 60
Supported Interfaces 60
Provisioning RACF 60
Provisioning RACF for a Subscriber 62
Provisioning an Authorization Code 62

Resource Reservation Protocol 63
Prerequisites 63
Supported Interfaces 63
Provisioning the RSVP 63

Screen List Editing 63
Prerequisites 63
Supported Interfaces 63
Provisioning SLE 64
Provisioning SLE for Subscribers, Centrex, and MLHG 66
Provisioning SCF,SCR, SCA and DRCW — Alternative Method 66

Selective Call Acceptance 67
Prerequisites 67
Supported Interfaces 67
Provisioning SCA 67
Provisioning SCA for Centrex 68
Selective Call Forwarding 68
  Prerequisites 68
  Supported Interfaces 68
  Provisioning SCF 68
  Provisioning SCF for Centrex 69
Selective Call Reject 69
  Prerequisites 69
  Supported Interfaces 69
  Provisioning SCR 69
  Provisioning SCR for Centrex 70
Service Code 311: Non Emergency Service 70
  Prerequisites 70
  Supported Interfaces 71
  Provisioning Service Code 311: NES 71
Service Code 411: Directory Assistance 72
  Prerequisites 72
  Supported Interfaces 72
  Provisioning Service Code 411: DA 73
Service Code 611: Repair 73
  Prerequisites 74
  Supported Interfaces 74
  Provisioning Service Code 611: Repair 74
Service Code 711: Telecommunications Devices for the Deaf Relay 75
  Prerequisites 75
  Supported Interfaces 75
  Provisioning Service Code 711: TDD Relay 76
Service Code 811: Telco Business Office 77
  Prerequisites 77
  Supported Interfaces 77
  Provisioning Service Code 811: Telco Business Office 78
Service Code 911: Emergency 78
  Prerequisites 79
  Supported Interfaces 79
  Provisioning Service Code 911: Emergency 80
  Provisioning 911 Emergency Services for Centrex 80
Speed Dialing 80
<table>
<thead>
<tr>
<th>Feature</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>80</td>
</tr>
<tr>
<td>Supported Interfaces</td>
<td>81</td>
</tr>
<tr>
<td>Provisioning Speed Dialing</td>
<td>81</td>
</tr>
<tr>
<td>Provisioning Speed Dialing for Subscribers and MLHG</td>
<td>82</td>
</tr>
<tr>
<td>Provisioning Speed Dialing for Centrex</td>
<td>82</td>
</tr>
<tr>
<td>Split Numbering Plan Area</td>
<td>83</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>84</td>
</tr>
<tr>
<td>Supported Interfaces</td>
<td>84</td>
</tr>
<tr>
<td>Provisioning a Split NPA</td>
<td>85</td>
</tr>
<tr>
<td>T.38 Fax Relay</td>
<td>86</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>86</td>
</tr>
<tr>
<td>Supported Interfaces</td>
<td>86</td>
</tr>
<tr>
<td>Provisioning T.38 Fax Relay</td>
<td>87</td>
</tr>
<tr>
<td>Three-Way Calling</td>
<td>87</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>87</td>
</tr>
<tr>
<td>Supported Interfaces</td>
<td>87</td>
</tr>
<tr>
<td>Provisioning TWC</td>
<td>87</td>
</tr>
<tr>
<td>Three-Way Calling Deluxe</td>
<td>88</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>88</td>
</tr>
<tr>
<td>Supported Interfaces</td>
<td>88</td>
</tr>
<tr>
<td>Provisioning TW CD</td>
<td>88</td>
</tr>
<tr>
<td>Provisioning TW CD for Centrex, and MLHG</td>
<td>88</td>
</tr>
<tr>
<td>Time and Weather</td>
<td>89</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>89</td>
</tr>
<tr>
<td>Supported Interfaces</td>
<td>89</td>
</tr>
<tr>
<td>Provisioning TW</td>
<td>89</td>
</tr>
<tr>
<td>Unified Messaging</td>
<td>90</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>90</td>
</tr>
<tr>
<td>Supported Interfaces</td>
<td>90</td>
</tr>
<tr>
<td>Provisioning Unified Messaging</td>
<td>90</td>
</tr>
<tr>
<td>Usage-Sensitive Three-Way Calling</td>
<td>91</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>91</td>
</tr>
<tr>
<td>Supported Interfaces</td>
<td>91</td>
</tr>
<tr>
<td>Provisioning USTWC</td>
<td>91</td>
</tr>
<tr>
<td>Provisioning USTWC for Subscribers and Centrex</td>
<td>92</td>
</tr>
<tr>
<td>Warmline</td>
<td>92</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>92</td>
</tr>
<tr>
<td>Supported Interfaces</td>
<td>92</td>
</tr>
<tr>
<td>Provisioning Warmline</td>
<td>92</td>
</tr>
</tbody>
</table>
Provisioning Warmline for Subscribers, Centrex, and M LHG 93

CHAPTER 7
Provisioning Announcements 1
Prerequisites 3
Supported Interfaces 3
Entering Gateway Information into the Cisco BTS 10200 Softswitch 3
Entering an Announcement and Release Cause 5
Creating Custom Announcements 5
Creating the Announcement and Downloading to the Cisco AS5300 5
Entering Announcement Data for a Custom Announcement 6
Cause Codes and Conditions 6
Prerecorded Announcements 7

CHAPTER 8
Provisioning SS7 1
Building the SS7 Network Configuration 1
Logging On to the Call Agent (Windows Environment) 2
Launching the JavaSoft Program 3
Creating a Local Point Code 4
Creating a Linkset 6
Creating a Signaling Link 8
Creating a Combined Linkset 11
Creating a Route Set 13
Creating a Global Title Translation 16
Alternate Provisioning for Automatic Callback and Automatic Recall Services 19
Termhandler 20
Provisioning the Cisco BTS 10200 Softswitch 25
SS7 Trunk Group Status and Control 27

CHAPTER 9
Provisioning and Troubleshooting ISDN 1

CHAPTER 10
Provisioning Analog Direct Inward Dial for PBXs 1

CHAPTER 11
Provisioning Channel-Associated Signaling 1
CAS Blocking 1
MS Package 2
DT Package 2
Provisioning CAS Trunk Groups 2
Media Gateway Setup for CAS 4
CAS Trunk Group Control Commands 5
- Bring the Media Gateway In Service 5
- Bring the CAS Trunk Group In Service 5
- Equip the CAS Trunk Terminations 6
- Bring the CAS Trunk Terminations In Service 6
    Troubleshooting Procedures 7

CHAPTER 12
Provisioning PacketCable 1

CHAPTER 13
Provisioning Trunk Groups 1

Provisioning Trunk Groups 1

CHAPTER 14
Provisioning CALEA 1

Provisioning CALEA 1

Security 1
- Service Independent Interception Provisioning 2
- PacketCable Electronic Surveillance Provisioning 2

CHAPTER 15
Digit Manipulation 1

Digit Manipulation 1

Overview 2
- Digit Manipulation Tables 8
  Pre-Translations Stage 10
  - Determining NOA for China 11
  - Digit Manipulation Profile Table 11
  - Digit Manipulation Table 12
  - Dial Plan Profile Table 14
  - International Dial Plan Profile Table 15
- Translations Stage 16
  - Dial Plan Table 16
  - International Dial Plan Table 18
- Routing Stage 19
  - Destination Table 19
  - Route Table 22
  - Trunk Group Table 27
- Delete Digits Function 31
  - Deletion of Leading Digits 32
  - Deletion of Specific Leading Digits 32
  - Deletion of Trailing Digits 32
  - Deletion of Specific Trailing Digits 32
<table>
<thead>
<tr>
<th>Feature Function</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deletion of Leading Digits if Length Matches</td>
<td>33</td>
</tr>
<tr>
<td>Deletion of Trailing Digits if Length Matches</td>
<td>33</td>
</tr>
<tr>
<td>Prefix Digits Function</td>
<td>33</td>
</tr>
<tr>
<td>Prefixing Leading Digits</td>
<td>33</td>
</tr>
<tr>
<td>Prefixing Leading Digits if Length Matches</td>
<td>34</td>
</tr>
<tr>
<td>Replace Digits Function</td>
<td>34</td>
</tr>
<tr>
<td>Replacing Leading Digits</td>
<td>34</td>
</tr>
<tr>
<td>Replacing Trailing Digits</td>
<td>35</td>
</tr>
<tr>
<td>Replacing Specific Digits</td>
<td>35</td>
</tr>
<tr>
<td>Replacing Leading Digits if Length Matches</td>
<td>35</td>
</tr>
<tr>
<td>Replacing Specific Digit Positions</td>
<td>35</td>
</tr>
<tr>
<td>Replacing Specific Digits by Position</td>
<td>36</td>
</tr>
<tr>
<td>Replace if Input String NULL</td>
<td>36</td>
</tr>
<tr>
<td>Nature of Address (NOA) Manipulation</td>
<td>36</td>
</tr>
<tr>
<td>Sample Provisioning</td>
<td>37</td>
</tr>
<tr>
<td>Feature Interaction</td>
<td>38</td>
</tr>
<tr>
<td>Glossary</td>
<td>38</td>
</tr>
</tbody>
</table>

**Chapter 16: Maintenance and Administration: System Components**

<table>
<thead>
<tr>
<th>Component</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>States</td>
<td>1</td>
</tr>
<tr>
<td>Returnable Status States</td>
<td>1</td>
</tr>
<tr>
<td>Returnable Control States</td>
<td>3</td>
</tr>
<tr>
<td>Success and Failure Responses</td>
<td>3</td>
</tr>
<tr>
<td>Status Application Command</td>
<td>3</td>
</tr>
<tr>
<td>Control Application Command</td>
<td>3</td>
</tr>
<tr>
<td>Call Agent</td>
<td>4</td>
</tr>
<tr>
<td>Status Command</td>
<td>4</td>
</tr>
<tr>
<td>Control Command</td>
<td>4</td>
</tr>
<tr>
<td>Feature Server</td>
<td>5</td>
</tr>
<tr>
<td>Status Command</td>
<td>5</td>
</tr>
<tr>
<td>Control Command</td>
<td>5</td>
</tr>
<tr>
<td>Element Management System</td>
<td>5</td>
</tr>
<tr>
<td>Status Command</td>
<td>5</td>
</tr>
<tr>
<td>Control Command</td>
<td>6</td>
</tr>
<tr>
<td>Bulk Data Management System</td>
<td>6</td>
</tr>
<tr>
<td>Status Command</td>
<td>6</td>
</tr>
<tr>
<td>Control Command</td>
<td>6</td>
</tr>
<tr>
<td>Status System</td>
<td>7</td>
</tr>
</tbody>
</table>
# CHAPTER 17  
**Maintenance and Diagnostics: External Resources**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregation Status</td>
<td>2</td>
</tr>
<tr>
<td>ISDN Switchover</td>
<td>2</td>
</tr>
<tr>
<td>Media Gateway</td>
<td>3</td>
</tr>
<tr>
<td>Status Command</td>
<td>3</td>
</tr>
<tr>
<td>Control Command</td>
<td>3</td>
</tr>
<tr>
<td>Trunk Group</td>
<td>4</td>
</tr>
<tr>
<td>Status Command</td>
<td>5</td>
</tr>
<tr>
<td>Control Command</td>
<td>6</td>
</tr>
<tr>
<td>Subscriber Termination</td>
<td>7</td>
</tr>
<tr>
<td>Status Command</td>
<td>10</td>
</tr>
<tr>
<td>Single Subscriber Termination Status</td>
<td>10</td>
</tr>
<tr>
<td>All Subscriber Terminations Status</td>
<td>10</td>
</tr>
<tr>
<td>Administrative State Token</td>
<td>11</td>
</tr>
<tr>
<td>Operating State Token</td>
<td>11</td>
</tr>
<tr>
<td>Source Token</td>
<td>12</td>
</tr>
<tr>
<td>Control Command</td>
<td>12</td>
</tr>
<tr>
<td>Control a Gateway In Service</td>
<td>12</td>
</tr>
<tr>
<td>Control All Subscriber Terminations</td>
<td>13</td>
</tr>
<tr>
<td>Equip Command</td>
<td>13</td>
</tr>
<tr>
<td>Unequip Command</td>
<td>13</td>
</tr>
<tr>
<td>Trunk Termination</td>
<td>14</td>
</tr>
<tr>
<td>Status Command</td>
<td>16</td>
</tr>
<tr>
<td>Trunk Termination Status</td>
<td>16</td>
</tr>
<tr>
<td>Tokens</td>
<td>17</td>
</tr>
<tr>
<td>Control Command</td>
<td>19</td>
</tr>
<tr>
<td>Control One Trunk Termination</td>
<td>19</td>
</tr>
<tr>
<td>Control All Trunk Terminations</td>
<td>19</td>
</tr>
<tr>
<td>Reset Command</td>
<td>20</td>
</tr>
<tr>
<td>Reset a Single CIC</td>
<td>20</td>
</tr>
<tr>
<td>Reset a Range of CICs</td>
<td>20</td>
</tr>
<tr>
<td>Reset All CICs</td>
<td>21</td>
</tr>
<tr>
<td>Equip Command</td>
<td>21</td>
</tr>
<tr>
<td>Unequip Command</td>
<td>22</td>
</tr>
<tr>
<td>Diagnostic Tests</td>
<td>22</td>
</tr>
<tr>
<td>Media Gateway Tests</td>
<td>22</td>
</tr>
<tr>
<td>Subscriber Termination Tests</td>
<td>23</td>
</tr>
<tr>
<td>Trunk Termination Tests</td>
<td>24</td>
</tr>
<tr>
<td>SS7 Trunk Termination Tests</td>
<td>24</td>
</tr>
</tbody>
</table>
## ISDN Trunk Termination Tests 25
- CAS Trunk Termination Tests 25
- Announcement Trunk Termination Tests 26

## Command Responses 26
- Generic Responses to Status or Control Command Failures 26
- Generic Success and Failure Responses 27
- System Error Response 28
- Termination Reason Responses 28
- Trunk Reason Responses 29
- Fault Reason Responses (Release 3.3) 30

### Chapter 18: Managing Billing Interface and Billing Records 1
- Record Retention Mechanisms in the EMS 1
- Billing Alarm Tracking Mechanisms 1
- Call Detail Block Correlation and Format 2
- Northbound Billing Data Transport 2

### Chapter 19: Traffic Measurements 1
- Traffic Management Subsystem 1
- Filtering Traffic Measurements 1
- Retrieving Traffic Measurement Summaries 2
- Format of Traffic Measurement Summaries 3
- List of Traffic Measurements (Counters) 4
  - Resources and Definitions 4
  - CA and POTS FS Measurement Counters for SIP Messages and Subscriber Features 5
  - Subscriber Feature Measurement Counters for AIN FS 20
  - Service Interaction Manager Counters 26
  - M GCP Adapter Measurement Counters 31
  - ISUP Measurement Counters 32
  - Call Processing Measurement Counters 35
  - H.323 Protocol Measurement Counters 42
  - SIP-T Adapter Measurement Counters 47
  - ISDN Measurements 51
  - Billing Measurement Counters 53
  - SNMP Measurements 55
  - Trunk Group Usage Measurement Counters 56
  - Announcement Measurement Counters 57
CHAPTER 20
Audit Database and Table Name

Audit Database
Table Name

CHAPTER 21
Database Usage

Show
Change

CHAPTER 22
Transactions

Transaction Queue
Show
Delete
Queue Throttle

CHAPTER 23
History

Show
Report

CHAPTER 24
Call Trace Summary

CHAPTER 25
Command Scheduler

Show
Add
Change
Delete

CHAPTER 26
Backing Up and Restoring the Cisco BTS 10200 Softswitch

Back Up the Cisco BTS 10200 Softswitch
Remote Network File Server Preparation
Log In to the Standby Cisco BTS 10200 Softswitch
Terminate All Applications on the Standby Cisco BTS 10200 Softswitch
Run a Backup of the Cisco BTS 10200 Softswitch
Activate All Applications on the Standby Cisco BTS 10200 Softswitch
Use FTP to Back Up Files to a Remote NFS
Compare Checksums
Managing Files In the Backup Directory
Backing Up Ulticom OMNI Data
Automatic Backup
Contents

Important Notes About This Procedure 7
Operator Backup 7
Starting the OMNI Stack 7
Execute Backup Command 8
Restoring the Cisco BTS 10200 Softswitch 9
  Restore Primary Cisco BTS 10200 Softswitch Shared Memory Data 9
  FTP Backup Files to the Primary Cisco BTS 10200 Softswitch 9
  Verify That Files Are Transferred 10
  Performing Shared Memory Restore 11
Start Platforms 11
Check System Status 12
  Log In to the Primary EMS for CLI Session 12
  Check for Alarms on the System 13
Restoring Ulticom Omni Data 14
  Important Notes About This Procedure 14
Restore Procedure 14
  Log In to the Active CA as Root User 14
  Stop the Application and Delete the Existing Configuration 14
  Start the Omni Stack and Restore Omni Data from the Backup File 15
  Start the Cisco BTS 10200 Softswitch Application 16
Preface

This document describes the steps used to provision and maintain the Cisco BTS 10200 Softswitch Call Agent (CA), Feature Server (FS), Element Management System (EMS), and Bulk Data Management System (BDMS) for Release 3.5.2 and 3.5.3. Basic hardware and operator interfaces are also covered.

Audience

This guide is designed for Cisco BTS 10200 Softswitch users and system administrators.

Modification History

The following modifications were made to this document since the last release. It is not an inclusive list.

- Chapter 1: Updated Hardware and Rack Configuration sections. Added Hardware Monitoring and Alarm Panel information. Updated the procedures for replacing a disk.
- Chapter 2: Updated Operator Interfaces section. Removed references to Telnet, added Secure Shell.
- Chapter 3: New
- Chapter 4: Reorganized and updated entire chapter.
- Chapter 5: Added Equal Access provisioning. Updated Call Agent section.
- Chapter 6: Updated entire chapter.
- Chapters 7 through 11: Updated and reorganized. Termhandler information added to Chapter 8.
- Chapter 12: New
- Chapter 13: Updated
- Chapters 14 and 15: New
- Chapter 16: Updated status and control command usage, added BDMS commands.
- Chapter 17: Updated status and control command usage, added command responses.
- Chapter 18: Updated and reorganized.
- Chapter 19: Updated
- Chapters 20 through 25: New
- Chapter 21: Updated
- Updated Call Trace Summary in Chapter 24. No HTML report is generated.
• Changed Calling Name Delivery Blocking description.
• Added procedure for Calling Number Delivery Blocking.
• Added note to Chapter 8 regarding the “unknown” state when provisioning SS7 trunks.
• Added disk replacement procedure to Chapter 1: Hardware.
• Added procedure for alternate Omni provisioning method for automatic callback and automatic recall.

Document Organization

This document is organized as follows:
• Chapter 1, “Hardware”
• Chapter 2, “Operator Interfaces”
• Chapter 3, “Provisioning External Media Gateways”
• Chapter 4, “Managing Access and Users”
• Chapter 5, “Provisioning the Call Agent, Subscribers, and Equal Access”
• Chapter 6, “Provisioning Features and Services”
• Chapter 7, “Provisioning Announcements”
• Chapter 8, “Provisioning SS7”
• Chapter 9, “Provisioning and Troubleshooting ISDN”
• Chapter 10, “Provisioning Analog Direct Inward Dial for PBXs”
• Chapter 11, “Provisioning Channel-Associated Signaling”
• Chapter 12, “Provisioning PacketCable”
• Chapter 13, “Provisioning Trunk Groups”
• Chapter 14, “Provisioning CALEA”
• Chapter 15, “Digit Manipulation”
• Chapter 16, “Maintenance and Administration: System Components”
• Chapter 17, “Maintenance and Diagnostics: External Resources”
• Chapter 18, “Managing Billing Interface and Billing Records”
• Chapter 19, “Traffic Measurements”
• Chapter 20, “Audit Database and Table Name”
• Chapter 21, “Database Usage”
• Chapter 22, “Transactions”
• Chapter 23, “History”
• Chapter 24, “Call Trace Summary”
• Chapter 25, “Command Scheduler”
• Chapter 26, “Backing Up and Restoring the Cisco BTS 10200 Softswitch”
Notes, Cautions, Warnings, and Tips

Notes, cautions, warnings, and tips are used throughout the document where applicable.

**Note**
Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

**Tip**
Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information or information that might save time.

**Caution**
Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Warning**
Means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translated versions of the warning, refer to the Regulatory Compliance and Safety document that accompanied the device.

Conventions

The following conventions apply to the commands:

- All commands start with a verb.
- A noun immediately follows the verb if appropriate.
- All primary keys must be specified in add, change, or delete commands.
- A primary key cannot be changed—it identifies the record.
- All parameters must be specified in a “token-name=value” pair. However, when a parameter (token) is referenced by another table, a full table-name qualifier is required. For example, in the Local Service Area table, the token is ID, but since the table is referenced by the LSA Profile table, the command is entered as lsa-id. Likewise, the token is also specified as lsa-id when used in the LSA Profile table.
- Each value is terminated by a semicolon.
- A token can contain several values separated by commas.
- All token names, command verbs, and command nouns are case insensitive.
- All values entered after the equal sign (=) in a command are case sensitive.

**Caution**
You must enter system component names in the case in which they were originally added to the system. For example, if a Call Agent ID was entered in lowercase (ca146), you must always enter it in lowercase. If it was entered in uppercase (CA146), you must always enter it in uppercase or you will get an error.
message. Likewise, feature tokens are always entered in uppercase, or you will receive the message “Reply: Database is void of entries.” For example, enter AC_ACT, not ac_act.

- White space is allowed in a value field if the value type is an ASCII character string.
- Any alphanumeric character and spaces can be used in specified values.
  - All fields that are alphanumeric characters by definition are stored in string form in the database.
  - If a token has a default value, the value is considered optional when entering a command. However, the token itself can be required, but its default value is automatically entered into the system.
  - Optional fields can become required based on the provisioning of another token. For example, in the Destination Table, Carrier-id (optional) becomes required if route-type=Carrier.
  - All fields that represent digit strings are entered and displayed in the proper dial plan format with a dash (-) but only the numeric characters are stored in the database. The international dial-plan digits should not contain dashes.
  - All dashes (-) in the token fields are converted to underscores (_) when they are stored in the database.

⚠️ **Caution**

Exception—feature tokens must be typed with an underscore (_) or you will receive the message “Reply: Database is void of entries.” For example, enter AC_ACT, not AC-ACT.

---

**Obtaining Documentation**

The following sections provide sources for obtaining documentation from Cisco Systems.

**World Wide Web**

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- [http://www.cisco.com](http://www.cisco.com)
- [http://www-china.cisco.com](http://www-china.cisco.com)
- [http://www-europe.cisco.com](http://www-europe.cisco.com)

**Documentation CD-ROM**

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

**Ordering Documentation**

Cisco documentation is available in the following ways:
• Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:
  http://www.cisco.com/cgi-bin/order/order_root.pl
• Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
  http://www.cisco.com/go/subscription
• Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click Feedback in the toolbar and select Documentation. After you complete the form, click Submit to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn: Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.
Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:
http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:
• P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
• P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:
http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:
http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

P1 and P2 level problems are defined as follows:
• P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
• P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.
Hardware

This chapter describes aspects of the Cisco BTS 10200 Softswitch hardware, such as powering on and off the Cisco BTS 10200 rack system, monitoring the hardware, and using the system Alarm Panel. This information applies to Cisco BTS 10200 Softswitch systems residing within a Continuous Computing System rack, although other vendors are supported.

Rack Configuration

This section describes the layout of the Element Management System (EMS), Bulk Data Management System (BDMS), Call Agent (CA), and Feature Server (FS) in the Cisco BTS 10200 Softswitch rack system from Continuous Computing as Field Replaceable Units (FRUs). There are two sets of the units in the rack. One unit is located in the bottom half of the rack and the other is in the top half of the rack. The top half of the rack contains the primary CA/FS and the Primary EMS/BDMS. The bottom half of the rack contains the secondary CA/FS and the secondary EMS/BDMS. The two halves are separated by two Catalyst Ethernet switches.

The Call Agent field replaceable unit (FRU) looks like the one in the bottom half of Figure 1-1. It is slightly larger than the EMS FRU, which is also shown in Figure 1-1. On the front face of every Continuous Computing System is an LCD display. The display shows the current status of the system and shows any problems or failures with the FRU. The display is important when determining if the FRU is powered on or off. A silver switch to the left of the LCD powers the FRU on and off. Figure 1-1 shows the front face of a typical rack configuration.
Legend:
1. Alarm Panel, PDU power feed 8A
   Filler Panel
   PDU (DC systems)
2. Filler Panel
3. EMS/BDMS B
   CCN node address = 1
   PDU power feed 1A/1B
4. Field Replacement Unit (FRU)
5. CA/FS B
Powering On and Off

This section describes how to power on and off the Cisco BTS 10200 Softswitch.

Power On Procedure

This section describes how to power on the Cisco BTS 10200 rack system.

Note

Boot completion times vary with system type (CA/EMS) as well as size of database.

Step 1

Ensure that all power cables are properly fastened to the back of all the systems in the Cisco BTS 10200 rack system.

Step 2

Power on the Catalyst switch routers by plugging them into a viable power source.

Note

The Catalyst switch routers do not have a power button.

Step 3

On the front side of the rack system, power on the primary and secondary EMS by pulling on the silver knob to the left of the LCD and putting it in the ON position.

When you hear the fans operate on the unit, you can release the knob to its neutral position.

Step 4

Power on the CA and FS units by pulling on the silver knob to the left of the LCD and putting it in the ON position.

When you hear the fans operate in the unit, you can release the knob to its neutral position.

The Cisco BTS 10200 rack system is now powered on.
Power Off Procedure

This section describes how to power off the Cisco BTS 10200 rack system.

**Note**
The shutdown order is: secondary EMS, secondary CA, primary CA, and then primary EMS.

**Step 1**
Check the status of your system and ensure that the primary CA and primary EMS are active, and that the secondary CA and secondary EMS are in standby.

**Step 2**
Log in to the primary CA, secondary CA, primary EMS, and secondary EMS using SSH.

**Step 3**
To begin the platform shutdown process, enter the following in each window:

```
platform stop all <return>
```

**Caution**
Cisco recommends that you deactivate any SS7 links that are homed off of the unit before you begin the platform shutdown. For example, if you enter `platform stop all` on the secondary side, take down the links on the secondary side first. If you are unsure which links are homed on the primary side and which are homed on the secondary side, contact Cisco TAC for assistance. Once the maintenance is complete, reactivate the links after the Call Agent and Feature Server applications are back in service.

When the prompt returns to #>, the operating system is ready for shutdown.

**Step 4**
To shut down the FRUs, enter the following in each window of each node:

```
init 5 <return>
```

The unit is ready to power off when the LCD on the FRU reads “HALTED” or “Coma.”. When all the FRUs have reached the Halted or Coma state, continue to the next step.

**Step 5**
Power off the primary and secondary Call Agents and Feature Server by pulling on the silver knob to the left of the LCD and putting it in the OFF position.

When you hear the fans turn off in the unit, you can release the knob to its neutral position.

**Step 6**
Power off the primary and secondary EMS by pulling on the silver knob to the left of the LCD and putting it in the OFF position.

When you hear the fans turn off in the unit, you can release the knob to its neutral position.

**Step 7**
To power off the Catalyst switch routers, unplug the unit from its power source.

**Note**
The Catalyst switch routers do not have a power button.

The Cisco BTS 10200 rack system is now powered off.
Hardware Monitoring

The hardware monitor (HMN) subsystem monitors the CPUs, memory consumption, disk, and disk control utilization. The HMN subsystem also returns information and alarms as appropriate.

CPU

The HMN monitors one or more CPUs on a physical node and reports the following:

- Percentage of CPU idle
- Percentage of CPU in system mode
- Percentage of CPU in user mode
- Percentage of CPU in blocked I/O

Memory Consumption

The HMN monitors memory consumption and reports the following:

- Total “real” memory
- Free memory available
- Total swap space
- Free swap space available

Disk and Disk Utilization

The HMN monitors the disk and disk control utilization on a physical disk and controller level. This measurement is dependent on the driver support supplied for the SCSI controller from the vendor.

Note

The device names follow those of a Solaris kernel. These vary from device to device. A physically understandable “mapping” of these devices may be required.

The HMN reports the following for disk and disk control utilization:

- Utilization of disk devices (sd0, sd1, and so on)
- Transfer rates, transactions per second (TPS) and hard or soft errors

Alarm Reports

The HMN monitors the top ten processes in the system. These processes are tracked based on the amount of CPU time they consume. This is a measure over time where a process can start running hot. This monitor function does not report transient spikes in CPU usage by any individual process.

The HMN generates Alarm Reports on devices and facilities that exceed their default settings. Default settings can be adjusted to fit a specific set of customer requirements.
Alarms are generated under the following conditions:

- A process exceeds 70 percent of the CPU.
- The CPU is over 90 percent busy (10 percent idle).
- The load average exceeds 5 for at least a 5-minute interval.
- Memory is 95 percent exhausted and swap is over 50 percent consumed. This indicates the system is spending excessive time in paging virtual memory.
- A partition that is 50 percent consumed generates a minor alarm.
- A partition that is 70 percent consumed generates a major alarm.
- A partition that is 90 percent consumed generates a critical alarm.

The following hardware monitoring commands apply to Release 3.5.2/3. Refer to the Cisco BTS 10200 Command Line Interface Reference Guide for complete descriptions and usage of command tokens.

The show node command displays the current status of a Unix service on a particular node. Use the following example to show the status of a node:

```
show node node=CA146; service=telnet
```

The change node command alters the status of a Unix service on a particular node. Use the following example to change the status of a node:

```
change node node=CA146; service=ftp; enable=Y;
```

**Caution**

Altering these features after the delivery of a Cisco BTS 10200 Softswitch can create security issues in your network.

The control node command performs either a halt or reboot of the Unix operating system on a particular node. Use the following example to control a node:

```
control node node=CA146; action=HALT;
```

**Caution**

Change and report node are low-level maintenance activities. Execute with extreme caution.

After halting a Cisco BTS 10200 Softswitch node, you may need local console access or a power cycle to restart the node.

Use the following command to report the condition of a node:

```
report node node=CA146
```

The status node command provides a detailed report of the Cisco BTS 10200 Softswitch applications on a particular node. Use the following command to show the status of a node and its components:

```
status node node=CA146;
```

**Alarm Panel**

Disk Replacement

This section describes how to replace a defective disk on the Cisco BTS 10200 Softswitch. This procedure contains the following sections:

- Before You Start
- Replacing Disk 0 on CA/FS and EMS
- Replacing Disk 1 on CA/FS and EMS

Before You Start

Perform the following before replacing a disk:

- Identify the disk that needs to be replaced by viewing the `/var/adm/messages` file.
- Cisco recommends that either the new disk and the defective disk have the same part number or the size of the replacement disk be equal or larger than the defective disk size.
- Perform a Flash Archive procedure.

Replacing Disk 0 on CA/FS and EMS

Note

The letter “x” in cxt0d0 or cxt1d0 throughout the procedure refers to the SCSI controller ID of the system (either 0 or 1). Use the `format` command to find out the SCSI controller ID.

Step 1

Log in as root.

Note

If this node is primary, then you must change the state of the nodes to forced standby active.

Step 2

If this node is CA/FS, deactivate the Omni SS7 links. Run the “Deactivating and Activating Omni” procedure on page 1-14.

If this node is not CA/FS, proceed to Step 3.

Step 3

If this node is an EMS, back up the `/data1/oradata` directory on EMS only. Enter the following commands:

```
<hostname> # platform stop all
<hostname> # sync; sync
```

Step 4

Perform the following additional steps to back up the `/data1/oradata` directory on EMS:

```
<hostname> # tar -cf - /data1/oradata | gzip -fast - >/opt/data.bak.tar.gz
```

Step 5

Delete the Sun Disk Suite metadatabase. Enter the following command:

```
<hostname> #/usr/sbin/metadb -d -f cxt0d0s4 cxt1d0s4
```

Step 6

Save the system files. Enter the following command:

```
<hostname> # mount /dev/dsk/cxt1d0s0 /mnt
```
Step 7  Set up disk mirroring. Enter the following commands:

```
<hostname># cp /mnt/etc/system /mnt/etc/system.mirror
<hostname># cp /mnt/etc/vfstab /mnt/etc/vfstab.mirror
```

Step 8  Save the system files. Enter the following commands:

```
<hostname># mv /mnt/etc/rc3.d/S99platform /mnt/etc/rc3.d/saved.S99platform
<hostname># eeprom auto-boot?=false
```

Step 9  Change the system files to boot from Disk 1.

- **Edit the** `/mnt/etc/system` **file and remove the following lines, if present:**

```plaintext
# * Begin MDD root info (do not edit)
# forceload: misc/md_trans
# forceload: misc/md_raid
# forceload: misc/md_hotspares
# forceload: misc/md_mirror
# forceload: drv/pcipsy
# forceload: drv/simba
# forceload: drv/glm
# forceload: drv/md
# rootdev:/pseudo/md@0:0,2,blk
# * End MDD root info (do not edit)
# * Begin MDD database info (do not edit)
# set md:mddb_bootlist1="sd:244:16 sd:244:1050 sd:244:2084
# sd:260:16"
# set md:mddb_bootlist2="sd:260:1050 sd:260:2084"
# * End MDD database info (do not edit)
```

Step 10  Edit the `/mnt/etc/vfstab` file.

- **The following output is for CCPU and Sun Netra 1405 platforms:**

```plaintext
#device device mount FS fsck mount mount
#to mount to fsck point type pass at boot options
/
/dev/dsk/c1d0s2 /dev/rdsk/c1d0s2 /usr ufs 1 yes -
fd - /dev/fd fd - no -
/proc - /proc proc - no -
/dev/dsk/c0t1d0s3 - - swap - no -
/dev/dsk/c0t1d0s0 /dev/rdsk/c0t1d0s0 / ufs 1 yes -
/dev/dsk/c0t1d0s1 /dev/rdsk/c0t1d0s1 /var ufs 1 yes -
/dev/dsk/c0t1d0s5 /dev/rdsk/c0t1d0s5 /opt ufs 2 yes -
swap - /tmp tmpfs - yes -
```

- **The following output is for Sun Fire 1280, V120, Netra 20, Netra 440 platforms:**

```plaintext
#device device mount FS fsck mount mount
#to mount to fsck point type pass at boot options
/
```

Note: Run `fsck -y /dev/rdsk/cxt1d0s0` if the file system cannot be mounted.
Step 11  Shut down the system. Enter the following commands:

```bash
<hostname>## sync
<hostname>## shutdown -y -g0 -i5
```

Step 12  Power off the system.

Step 13  Remove the bad disk (disk0).

Step 14  Insert the new Disk 0 into the slot and power on the system.

Step 15  At the ok> prompt, type the following:

```bash
boot disk1
```

**Note**  If necessary, run `fsck -y` on the file system that cannot be mounted.

Step 16  Log in as root.

Step 17  Verify that the system is booting up and all file systems are mounted.

Step 18  Partition all slices on Disk 0 exactly like Disk 1, label it, and exit.

If the replacement disk does not have the same Model number, use the `format` command to manually partition the new disk, as follows:

<table>
<thead>
<tr>
<th>Slice</th>
<th>Mount Point</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>/(root)</td>
<td>1500MB</td>
</tr>
<tr>
<td>1</td>
<td>/var</td>
<td>500MB</td>
</tr>
<tr>
<td>2</td>
<td>swap</td>
<td>2000MB</td>
</tr>
<tr>
<td>3</td>
<td>unassigned</td>
<td>16MB</td>
</tr>
<tr>
<td>4</td>
<td>/opt</td>
<td>The rest of the disk space</td>
</tr>
<tr>
<td>5</td>
<td>unassigned</td>
<td>16MB</td>
</tr>
<tr>
<td>6</td>
<td>unassigned</td>
<td>64MB</td>
</tr>
</tbody>
</table>

Step 19  Set up mirroring slices. Enter the following commands:

```bash
<hostname>## /usr/sbin/metadb -a -f -c 3 cxt0d0s4 cxt1d0s4
<hostname>## /usr/sbin/metainit -f d0 1 1 cxt0d0s0
<hostname>## /usr/sbin/metainit -f d1 1 1 cxt1d0s0
<hostname>## /usr/sbin/metaroot d2
<hostname>## /usr/sbin/lockfs -fa
<hostname>## /usr/sbin/metainit -f d12 1 1 cxt0d0s6
<hostname>## /usr/sbin/metainit -f d13 1 1 cxt1d0s6
<hostname>## /usr/sbin/metainit d14 -m d13
<hostname>## /usr/sbin/metainit -f d9 1 1 cxt0d0s5
<hostname>## /usr/sbin/metainit -f d10 1 1 cxt1d0s5
<hostname>## /usr/sbin/metainit d11 -m d10
<hostname>## /usr/sbin/metainit -f d3 1 1 cxt0d0s1
<hostname>## /usr/sbin/metainit -f d4 1 1 cxt1d0s1
<hostname>## /usr/sbin/metainit d5 -m d4
<hostname>## /usr/sbin/metainit -f d6 1 1 cxt0d0s3
<hostname>## /usr/sbin/metainit -f d7 1 1 cxt1d0s3
```
Replacing Disk 0 on CA/FS and EMS

Chapter 1      Hardware

Replacing Disk 0 on CA/FS and EMS

Step 20  Sync Disk 0 and Disk 1. Log in as root and enter the following commands:

<hostname>#/usr/sbin/metainit d8 -m d7
<hostname>#/usr/sbin/metainit -f d15 1 1 cxt0d0s7
<hostname>#/usr/sbin/metainit -f d16 1 1 cxt1d0s7
<hostname>#/usr/sbin/metainit d17 -m d16
<hostname>#/usr/sbin/metainit -f d18 -t d14 d17
<hostname>#/usr/sbin/metainit -f d19 -t d5 d17
<hostname>#/usr/sbin/metainit -f d20 -t d11 d17
<hostname>#/etc/system.mirror /etc/system
<hostname>#/etc/vfstab.mirror /etc/vfstab
<hostname>##sync
<hostname>##halt
OK>boot disk1

Step 21  At this time, Disk 0 is synchronizing with Disk 1. The process will take a while.

Run `metastat|grep %` to monitor the percentage completion.

Note: Do not continue until the synchronizing process is 100% completed.

Step 22  Enter the following command:

<hostname>##metastat |grep cx

Step 23  Verify that all slices are okay.

Ex:     cxt0d0s6                   0     No    Okay
        cxt1d0s6                   0     No    Okay
        cxt0d0s1                   0     No    Okay
        cxt1d0s1                   0     No    Okay
        cxt0d0s5                   0     No    Okay
        cxt1d0s5                   0     No    Okay
        cxt0d0s7                   0     No    Okay
        cxt1d0s7                   0     No    Okay
        cxt0d0s0                   0     No    Okay
        cxt1d0s0                   0     No    Okay
        cxt0d0s3                   0     No    Okay
        cxt1d0s3                   0     No    Okay

Step 24  Once the synchronizing process is completed, reboot the system using disk0 to verify.

Step 25  Reboot the system. Enter the following commands:

<hostname>##sync
<hostname>##shutdown -y -g0 -i6

Step 26  Bring up all platforms and Omni SS7. Log in as root.

Step 27  Enter the following command:

<hostname>##platform start

Note: Run the procedures in Deactivating and Activating Omni, page 1-14, if this node is CA/FS.
Step 28  Restore the system files. Enter the following commands:

<hostname> # mv /etc/rc3.d/saved.S99platform /etc/rc3.d/S99platform
<hostname> # eeprom auto-boot?=true
<hostname> # rm /opt/data.bak.tar.gz (if this node is EMS).

Replacing Disk 1 on CA/FS and EMS

Note  The letter “x” in cxt0d0 or cxt1d0 throughout the procedure refers to the SCSI controller ID of the system (either 0 or 1). To find out the controller ID, use the format command.

Step 1  Log in as root.

Note  If this node is primary, you must change the state of the nodes to forced standby active.

Deactivate Omni SS7 links on CA/FS only.

Note  Run the procedures in Deactivating and Activating Omni, page 1-14, if this node is CA/FS.

Step 2  Back up the /data1/oradata directory on EMS only. Enter the following commands:

<hostname> # platform stop all
<hostname> # sync; sync

Step 3  If this node is an EMS, perform the following additional steps, otherwise go to Step 4.

<hostname> # tar -cf - /data1/oradata | gzip -fast - >/opt/data.bak.tar.gz

Step 4  Save the system files. Enter the following commands:

<hostname> # cp /etc/system /etc/system.mirror
<hostname> # cp /etc/vfstab /etc/vfstab.mirror
<hostname> # mv /etc/rc3.d/S99platform /etc/rc3.d/saved.S99platform
<hostname> # /usr/sbin/metadb -d -f cxt0d0s4 cxt1d0s4

Step 5  Change the system files to boot from Disk 0. Edit the /etc/system file and remove the following lines, if present:

* Begin MDD root info (do not edit)
  forceload: misc/md_trans
  forceload: misc/md_raid
  forceload: misc/md_hotspares
  forceload: misc/md_stripe
  forceload: misc/md_mirror
  forceload: drv/pcipsy
  forceload: drv/simba
  forceload: drv/glm
  forceload: drv/sd
  rootdev:/pseudo/md@0:0,2,blk
* End MDD root info (do not edit)
* Begin MDD database info (do not edit)
set md:mddb_bootlist1="sd:244:16 sd:244:1050 sd:244:2084"
Replacing Disk 1 on CA/FS and EMS

Chapter 1      Hardware

Step 6 Edit the /etc/vfstab file:

a. The following output is for CCPU and Sun Netra 1405 platforms:

```
#device device mount FS fsck mount mount
#/dev/dsk/c1d0s2 /dev/rdsk/c1d0s2 /usr ufs 1 yes -
#fd      -       /dev/fd fd      -       no -
#proc   -       /proc   proc    -       no -
/dev/dsk/c0t0d0s3 - - swap - swap - no -
/dev/dsk/c0t0d0s0 /dev/rdsk/c0t0d0s0 / / ufs 1 yes -
/dev/dsk/c0t0d0s1 /dev/rdsk/c0t0d0s1 /var ufs 1 yes -
/dev/dsk/c0t0d0s5 /dev/rdsk/c0t0d0s5 /opt ufs 2 yes -
swap   -       /tmp   tmpfs   -       yes -
```

b. The following output is for Sun Fire 1280, V120, Netra 20, Netra 440 platforms:

```
#device device mount FS fsck mount mount
#/dev/dsk/c1d0s2 /dev/rdsk/c1d0s2 /usr ufs 1 yes -
#fd      -       /dev/fd fd      -       no -
#proc   -       /proc   proc    -       no -
/dev/dsk/c1t0d0s3 - - swap - swap - no -
/dev/dsk/c1t0d0s0 /dev/rdsk/c1t0d0s0 / / ufs 1 yes -
/dev/dsk/c1t0d0s1 /dev/rdsk/c1t0d0s1 /var ufs 1 yes -
/dev/dsk/c1t0d0s5 /dev/rdsk/c1t0d0s5 /opt ufs 2 yes -
swap   -       /tmp   tmpfs   -       yes -
```

Step 7 Shut down the system. Enter the following commands:

```
<hostname>sync
<hostname>shutdown -y -g0 -i5
```

Step 8 Power off the system.

Step 9 Remove the defective disk (disk1).

Step 10 Insert the new disk1 into the slot and power on the system.

Note If necessary, run fsck -y on the file system that cannot be mounted.

Step 11 Verify that the system is booting up and all file systems are mounted.

Step 12 Partition Disk 1. Partition all slices on Disk 1 exactly like Disk 0, label it and exit.

If the replacement disk does not have the same Model number, use the format command to manually partition the new disk, as follows:

Slice 0  / (root)  1500MB
Slice 1  /var  500MB
Slice 3  swap  2000MB
Step 13  Set up mirroring slices and sync both Disk 0 and Disk 1. Perform the following steps to set up disk mirroring:

CA/FS:  cd /opt/setup
        ./setup_mirror_ca

Note  Ignore the error "mv: cannot access ./vfstab_mirror."

        ./setup_trans

Note  Ignore the error "mv: cannot access ./vfstab_trans."

cp /etc/system.mirror /etc/system
cp /etc/vfstab.mirror /etc/vfstab
sync
reboot
login as root
cd /opt/setup
./sync_mirror

EMS:  cd /opt/setup
./setup_mirror_ems

Note  Ignore the error "mv: cannot access ./vfstab_mirror."

        ./setup_mirror_trans

Note  Ignore the error "mv: cannot access ./vfstab_trans."

cp /etc/system.mirror /etc/system
cp /etc/vfstab.mirror /etc/vfstab
sync
reboot
login as root
cd /opt/setup
./sync_mirror

Step 14  At this time, Disk 1 is synchronizing with Disk 0. The process will take a while. Run `metastat|grep %` to monitor the percentage completed.

Note  Do not continue until the synchronizing process is 100% completed.

Step 15  Verify the mirroring process. Enter the following command:

<hostname>#metastat|grep cx
Step 16  Verify that all slices are okay.

Ex:
- cxt0d0s6                   0     No    Okay
- cxt1d0s6                   0     No    Okay
- cxt0d0s1                   0     No    Okay
- cxt1d0s1                   0     No    Okay
- cxt0d0s5                   0     No    Okay
- cxt1d0s5                   0     No    Okay
- cxt0d0s7                   0     No    Okay
- cxt1d0s7                   0     No    Okay
- cxt0d0s0                   0     No    Okay
- cxt1d0s0                   0     No    Okay
- cxt0d0s3                   0     No    Okay
- cxt1d0s3                   0     No    Okay

Step 17  Bring up all platforms. Enter the following command:

<hostname>#$platform start

Note  Run the procedures in Deactivating and Activating Omni, page 1-14, if this node is CA/FS.

Step 18  Restore the system files. Enter the following commands:

<hostname>#$mv /etc/rc3.d/saved.S99platform /etc/rc3.d/S99platform
<hostname>#$rm /opt/data.bak.tar.gz (if this node is EMS)

Deactivating and Activating Omni

The following steps apply only to CA/FS servers that use the Omni configuration.

Deactivating Omni

Deactivate the Omni SS7 links associated with this host.

Step 1  Log in as root.

Step 2  Enter the following commands:

<hostname>#$cd /opt/omni/bin
<hostname>#$termhandler -node a7n1
OMNI [date] #1:deact-slk:slk=LNK0;
OMNI [date] #2:deact-slk:slk=LNK1;

Step 3  Enter y to continue.

Step 4  Repeat Step 2 for each active link that is associated with this box ONLY.

Step 5  Enter the following command:

OMNI [date] #3:display-slk;

Step 6  Enter y to continue.

Step 7  Verify that the state for each link is INACTIVE.

Step 8  Enter the following command:
Activating Omni

Activate the Omni SS7 links associated with this host.

**Step 1** Log in as root.

**Step 2** Enter the following commands:

```
<hostname> cd /opt/omni/bin
<hostname> termhandler -node a7n1
OMNI [date] #1:actv-slk:slk=LNK0;
OMNI [date] #2:actv-slk:slk=LNK1;
```

**Step 3** Enter y to continue.

**Step 4** Repeat **Step 2** for each active link that is associated with this box ONLY.

**Step 5** Enter the following command:

```
OMNI [date] #3:display-slk;
```

**Step 6** Enter y to continue.

**Step 7** Verify that the state for each link is ACTIVE.

**Step 8** Enter the following command:

```
OMNI [date] #4:quit;
```
Operator Interfaces

This chapter describes the operator interfaces used for communication with the Cisco BTS 10200 Softswitch and contains the following sections:

- Logging in Using Secure Shell
- Bulk Provisioning
- EMS Services

The Element Management System (EMS) has the following external interfaces (see Figure 2-1) to support several types of communications:

- **Local operator console with the following options:**
  - Interactive command-line interface (CLI) session—Operator connects to the EMS using Secure Shell (SSH) and uses the CLI in an interactive session.
  - Menu Assisted Commands (MAC) session—Operator connects to the EMS using SSH and uses the MAC interface.
  - Maintenance (MAINT)—Operator connects to the EMS using SSH and uses the MAINT interface.
  - Bulk provisioning—Operator connects to the EMS using FTP for batch-mode provisioning (requires highest privilege levels).

*Note* After entering any of the commands in this chapter, press the Return or Enter key.

- Network management system—Provides events, alarms, thresholds, and traffic monitoring management commands into the EMS using the Simple Network Management Protocol (SNMP).
- Common Object Request Broker Architecture (CORBA) Client—Provides events, alarms, thresholds, and traffic monitoring management commands into the EMS using CORBA.

The EMS database holds up to 100 operator logins. Up to 50 user sessions can be active at any time. The EMS interfaces internally with the Call Agent (CA) and Feature Server (FS) using the Java Message Service (JMS) protocol over IP Protocol.
Logging in Using Secure Shell

This section describes how to log in to the Cisco BTS 10200 Softswitch using SSH. SSH is the method of access to the Cisco BTS 10200 Softswitch CLI, MAINT, or MAC. SSH provides encrypted communication between a remote machine and the EMS or Call Agent for executing CLI, MAINT, or MAC commands. The SSH server runs on the EMSs and CAs of the Cisco BTS 10200 Softswitch. To connect, the client and server sides must run the secure shell daemon (SSHD).

With SSH enabled, new users are prompted to enter a new password and reenter that password during their first login. From that point, they are prompted once for a password only.

Step 1
To log in from the client side, enter the following:

```
ssh username@IPaddress
```

On the first SSH login from the client side, expect a message similar to this:

```
The authenticity of host [hostname] can't be established.
Are you sure you want to continue connecting (yes/no)?
```

Step 2
Enter yes.

The default password prompt appears. From this point on, all communications are encrypted. Enter the default password.

Note
Subsequent SSH logins will prompt only for a password.
Step 3  At the login prompt, enter your CLI username.
The password prompt appears.

Step 4  Enter your password.
The system responds with a CLI> prompt. You are now ready to send commands to the EMS.

Step 5  Enter the desired provisioning commands.

Step 6  To log off, enter **exit** at the prompt.

---

**Bulk Provisioning**

Batch files can be prepared in advance and then forwarded using the Secure File Transfer Protocol (SFTP) to the EMS for execution. Cisco recommends that SFTP access be made available only to users with the highest privilege level. The user can make an SFTP connection and navigate to a dedicated batch provisioning directory in the EMS. Once there, the user can drop batch provisioning files in this directory. The directory is checked every 20 seconds for files. Each file is processed line by line as a series of separate commands. Once the file is processed, it is moved from that directory to the directory `/opt/ems/ftp/deposit`. A report file is created and viewable through a browser by going to location http://ems<MachineName or IP addr> :10200.

To communicate using SFTP, perform the steps in the following sections:

1. Preparing a Script File on your Local System, page 2-3
2. Connecting to the EMS, page 2-4
3. Transferring a Script File to the EMS, page 2-4
4. Confirming that a Script File Has Been Processed, page 2-5

**Preparing a Script File on your Local System**

A script file is a series of CLI commands that you want to enter into the system.

To prepare a script file, perform the following steps:

**Step 1**  On any computer, prepare and save a script file ASCII text format.

**Note**  The syntax of the files must follow that of the CLI. Enter each line in this file as it would be entered on the CLI. Blank lines are allowed and commented lines are allowed provided they begin with #. Use the VALIDATE keyword to verify syntax of commands without committing the commands to the database. (Refer to the *Cisco BTS 10200 Command Line Reference Guide* for command syntax and parameters.)

**Step 2**  Open a UNIX shell, or in Windows, open a DOS prompt or a command prompt window using cmd.exe.

**Step 3**  At the prompt, navigate to the directory containing the script file you created in Step 1.

For UNIX: cd <directory on your local system that contains the script file>
For DOS: cd <directory on your local system that contains the script file>
Connecting to the EMS

To connect to the EMS, perform the following steps:

Step 1  Ensure that you have TCP/IPC connectivity to communicate with the primary and secondary EMS units.

Step 2  At the local prompt, enter `sftp` and the domain name or IP address of the primary EMS.

```
sftp <username@DNS/IP Address>
```

The system responds with a login/user prompt.

Note  If the primary EMS is down, use SFTP to connect to the secondary EMS.

Step 3  Enter the username specified in Step 2.

The password prompt appears.

Step 4  Enter the password.

The system displays an sftp> prompt.

Step 5  Proceed to Transferring a Script File to the EMS.

Transfering a Script File to the EMS

To transfer a script file to the EMS, perform the following steps:

Step 1  Change the directory to the batch update location.

```
cd /opt/ems/ftp/deposit
```

Note  This is the EMS dedicated batch update directory. This directory name cannot be changed.

Step 2  Verify that you are in the correct directory.

```
pwd
```

Step 3  At the sftp prompt, enter `put` and the name of the ASCII script file to be sent.

```
put <file name>
```

Note  If the system cannot execute a command in the script, it will log the appropriate error message(s). After five errors the file aborts.

Step 4  Proceed to Confirming that a Script File Has Been Processed.
Confirming that a Script File Has Been Processed

Confirm that the system generated an output file by going to the following URL and opening the Bulk Provisioning Report file:

http://ems<MachineName or IP addr> :10200

This completes the steps for bulk provisioning.

EMS Services

This section describes EMS activity commands. EMS activity commands are available to manage the users and other services on the system. The activity timer for user sessions is not part of any schema or table. This is a system configuration parameter.

EMS Users and Services Commands

This section describes the EMS user and other service commands on the system.

Show

Use the following command example to show user activity on the EMS:

show ems;

Change

Use one of the following command examples to change a service on the EMS:

change ems interface=hma0;ip-alias=<the ip-address>
change ems ntp-server=ntp_server_1,ntp_server_2

EMS NTP Server Configuration

The network time protocol (NTP) is designed to synchronize the clocks of computers over a network. It uses multiple redundant servers in order to achieve high accuracy and reliability.

Use the following CLI command to configure the NTP server:

change ems ntp_server=<ntp_server_1>,<ntp_server_2>

where:

ntp_server_1 and ntp_server_2 are the IP addresses of reference time source servers.
Provisioning External Media Gateways

The Media Gateway Provisioning (MGP) command allows direct command access to a gateway, and is used to provision configurations on a gateway through the Cisco BTS 10200 Softswitch. After an MGP entry is added to the system, you can access the gateway via the escape command sequence at the CLI, FTP adapter, or by using the MGP object interface in the CORBA adapter.

This command applies only to the following media gateways:

- Cisco MGX 8260
- Cisco AS5850
- Cisco MGX 8850
- Cisco AS5400

**Step 1**

Use one of the following examples to show, add, change or delete an external media gateway.

```
show mgp

add mgp ip-addr=10.89.224.10; type=As5400; user-name=cisco; password=cisco123;
```

**Note**

After adding a gateway, use your applicable vendor documentation to configure the gateway using the escape command. The format for the escape command is: `mgp <IPaddress> gateway command`.

The `mgp` keyword indicates to the CLI that the command is not for the Cisco BTS 10200 Softswitch. It is to be sent to the gateway defined by the IP address. This is the same address as the one used to create the MGP entry in the `add mgp` command.

```
change mgp gateway1.cisco.com; password=cisco

delete mgp ip-addr=10.89.224.10;
```
Managing Access and Users

The security management system controls and monitors access to the Cisco BTS 10200 Softswitch from outside sources. This security system is important in preventing the following:

- Errors by personnel not trained in specific procedures
- Unauthorized changes to system provisioning
- Unauthorized viewing or modification of databases

Internal security functions include:

- Providing a user interface to provision users and security classes (privilege levels)
- Storing user login profiles
- Performing user authentication
- Managing the level of access on a per-user basis
- Providing session-oriented security measures
- Providing transaction-oriented security measures
- Logging all access activity to a log
- Maintaining security log for 7 days
- Providing a user interface for security log reporting

Note: Refer to the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide* for specific CLI commands and tokens.

User and Command Privilege Levels

Each command (verb-noun combination) is preassigned a security class of 1 to 10, with 1 being the lowest level and 10 the highest level. The security class indicates the minimum privilege level required for an operator to complete the command. The system administrator can assign an alphanumeric description with each of these security classes.

Note: The security classes are preassigned for each command, but can be changed by the system administrator.
The system administrator enters a new user and assigns a privilege level from 1 to 10 (level 10 is typically reserved for the system administrator). Each time a user enters a command, the system compares the user’s privilege level to the security class of the specific command. The command is denied if the user has a privilege level less than the command level.

The user interface of the security management system allows users with the highest privilege levels to perform the following security tasks:

- Enter users into the system database
- Assign or modify a user’s privilege level
- Reset the password of any user
- Modify descriptions of a security level
- Manage security log reporting and obtain security reports

### Command Level Provisioning

The Command Level (command-level) table identifies the ten command levels and their descriptions. The system is delivered with levels 1, 5 and 10 preset with descriptions. These are the lowest level, the mid level and the highest level administration access. Preset levels can be changed. Every security level can be assigned an alphanumeric description. The optional description token is intended for the service provider.

**Step 1**

To show a command level ID, use the following example:

```
show command-level id=10;
```

**Step 2**

To add a description to any command level ID, use the following example:

```
change command-level id=10; description=This is the highest level administration access;
```

### User Account Administration

A Cisco BTS 10200 Softswitch system is delivered with one account predefined as username=optiuser and password=optiuser. Cisco recommends resetting this password. New users can be added by this `superuser`. A new user who logs in for the first time is prompted to enter a new password and to reenter the new password for verification purposes. Passwords must be at least six characters in length and cannot contain the first three characters of the login name.

### Users

This section describes how to show, add, change and delete users.
Show, Add, Change, Delete

Users with privilege level 10 can add, change, delete and show data for a user identified as UserABC. Note that change user allows the privilege level of the user to be changed—but not the identity of the user. The days-valid and warn tokens specify the number of days a user’s password is valid, and the number of days warning the user receives before their password expires. The shell token can also be specified.

---

**Note**

After adding a new user to the system a default or initial password must be supplied with the following command:

```
reset password name=<user name>; new-password=<user password>
```

This is the standard Cisco BTS 10200 Softswitch command for the system administrator to reset a password.

---

**Step 1**
To show the details for a user, use the following example:

```
show user name=UserABC;
```

**Step 2**
To add a user, use the following example:

```
add user name=UserABC; command-level=9; warn=10; days-valid=30; workgroups=somegroup;
```

Reply Example:

Executing command, please wait...
Reply: Request was successfully completed

---

**Note**
The warn, days-valid, and workgroups tokens are optional.

---

**Step 3**
To change details for a specific user, use the following example:

```
change user name=UserABC; command-level=1; workgroups=somegroup;
```

Reply Example:

Executing command, please wait...
Reply: Request was successfully completed

---

**Note**
The change user command changes only the privilege level of the user, and not the identity of the user. The command-level and workgroups tokens are optional; however, one of them must be changed.

---

**Step 4**
To delete a user, use the following example:

```
delete user name=UserABC;
```

Reply Example:

Executing command, please wait...
Reply: Request was successfully completed
Invalid User Privilege Level

The following example shows what happens when a user with a privilege level less than 9 attempts to enter an add, show, change, or delete user command:

```plaintext
change user name=UserABC;command-level=6;
```

Reply Example:

```
Not authorized to execute change user:
User command-level: 2 level needed: 10
```

Caution

Never add, change, or delete the username `root`, because this affects proper access to the system.

User and Optiuser Set Password/Reset Password

The `password` command allows the system administrator to reset any user's password. It also allows setting the number of days that the password is valid and the number of days before password expiration that the user is warned. It also forces the system administrator to enter a new password. A user who logs in for the first time must execute this command again to change the password.

Users can reset only their own passwords. Users are allowed to reset the days a password is valid, the number of days before password expiration, and the user must enter a new password when executing this command.

Passwords must be constructed to meet the following UNIX standards:

- A password must be between 6 and 8 characters.
- A password must contain at least two alphabetic characters and at least one numeric or special character. In this case, alphabetic refers to all upper- or lowercase letters.
- A password must differ from the user's login name and any reverse or circular shift of that login name. For comparison purposes, an uppercase letter and its corresponding lowercase letter are equivalent.
- New passwords must differ from the old by at least three characters. For comparison purposes, an uppercase letter and its corresponding lowercase letter are equivalent.

The system default user/password combination for the CLI administrator is optiuser/optiuser. The username `optiuser` can never be deleted from the system. As a security measure, the system administrator should change the password for user `optiuser` on each system before deployment.

To change the password to optiuser, perform the following steps.

Note

Perform the same steps to change the password for any system user.

Step 1

Log on using SSH to one EMS unit with the username `optiuser` and the current password for optiuser.

```
ssh -1 <username> <ipaddress>
```

The CLI prompt appears.
Step 2  Enter the reset command:

```
reset password name=optiuser; new-passord=cisco4; days-valid=<number of days the new password will be valid>; warn=<number of days before password expiration to warn user>;
```

```
reset password name=optiuser; days-valid=45; warn=10;
```

Step 3  Enter exit to exit the CLI shell.

Step 4  Log on using SSH to the same EMS with user name optiuser.

The system prompts you for a new password.

Step 5  Enter the new password.

Step 6  The system prompts you for the new password again.

Step 7  Enter your new password.

The password for user optiuser is changed and the CLI prompt appears. You can continue with the CLI session if desired, or exit again.

---

**Command Table**

The Command Table (command-table) table allows a system administrator to show, change, and reset the command privilege level (CPL) of a specific noun-verb pair. This command requires a security level of 10 to execute. Security classes are preassigned for each command, but can be changed with the command-table command.

**Step 1**  To show the command privilege level of a specific noun-verb pair, use the following example:

```
show command-table noun=mgw; verb=add;
```

**Step 2**  To change the command privilege level of a specific noun-verb pair, use the following example:

```
change command-table noun=mgw; verb=add; sec-level=9;
```

**Step 3**  To reset the command privilege level of a specific noun-verb pair, use the following example:

```
reset command-table noun=mgw; verb=add;
```
Workgroups

Work-groups are created when you use the User or Command tables. The first time you use the work-groups token, you create the work-group and add the User/Command to the work-groups. Additional User/Commands are added to the work-groups the same way. The only exception is that the work-groups is already created.

The work-groups token is a logical collection of commands created by the service provider. Work-groups are valid only for the change command. An equal sign (=) without a plus sign (+) or minus sign (–) creates a new work-group. A plus sign (+) before the work-group name adds a work-group to a user. A minus sign (–) before the work-groups name removes a work-group from a user.

---

**Step 1**

To add a work-group for the first time, use the following example:

```bash
change command-table noun=mgw; verb=add; work-groups=latex;
```

Reply Example:

```bash
Reply : Success: Request was successfully completed
```

**Step 2**

To add one or more work-groups to an existing user, use the following example.

**Note** This does not replace any already existing work-groups.

```bash
change user name=trs80nut; work-groups=+rubber;
```

Reply Example:

```bash
Reply : Success: Request was successfully completed
```

**Step 3**

To remove one or more work-groups from an existing user, use the following example:

```bash
change user name=trs80nut; work-groups=-latex;
```

Reply Example:

```bash
Reply : Success: Request was successfully completed
```

---

Security Summary Report

The Security Summary command provides a summary report of security infractions by source and start/stop times from the Security Log (securitylog) table. The EMS maintains seven days of security infractions.

---

**Step 1**

To run a Security Summary report, use the following example:

```bash
report security-summary start-time=2002-09-26 00:00:00; end-time=2002-09-27 00:00:00; source=all;
```

**Note** If you enter this command without any tokens, the report shows all security infractions.
Step 2  Using the Cisco BTS 10200 Softswitch http:// server in an external browser (Netscape, Internet Explorer, and so forth), perform the following steps to retrieve the security-summary report file.

a. Enter the http:// server name.

   http://<your bts domain name>:10200>

b. Once on the main page, double-click the reports link.
   A set of directories appears.

   The security-summary log appears.

Example of Security Summary Report:
In the following example, user wwalbash, with a command-level 5 security level, tried to add a media gateway, which requires a security level of 8 or above. The attempt failed and is recorded in the Security Summary report for the Security manager.

```
report security-summary
```

Reply : Success: Request was successful.

```
USER=wwalbash
VERB=add
NOUN=mgw
DATE=2002-09-26 13:25:50.0
USER=wwalbash
VERB=add
NOUN=subscriber
DATE=2002-09-26 13:26:02.0
```

Session Manager

The Session Manager (SMG) user management tool tracks the session clients (users) that have logged in to the Cisco BTS 10200 Softswitch.

This section describes the session management activity commands. The stop, block, and unblock commands cannot be executed on the same terminal from which the command was entered. Command information in square brackets ([ ]) is mandatory. There is no mandatory information for the show command. Command information in curly braces ({ }) is optional.
Show Command

The show command queries all terminals in the system. The SMG returns a list of currently defined terminals. It allows the service provider to differentiate the list based on a user ID. If a terminal is not listed, all terminals are shown. The asterisk (*) wildcard is not supported.

Step 1

To query all terminals in the system, use the following example:

```
show session terminal={1-32 characters}
```

Reply Example:

```
Reply : Success

TERMINAL=USR5
USER=optiuser
STATE=ACTIVE
TYPE=CLI
TIME=2001-May-18 14:32:27

TERMINAL=USR4
USER=wenyang
STATE=ACTIVE
TYPE=CLI
TIME=2001-May-18 13:48:49

TERMINAL=USR3
USER=optiuser
STATE=ACTIVE
TYPE=CLI
TIME=2001-May-18 12:18:49

========= 
```

Block Command

The block command is executed on a single terminal ID. The terminal is then blocked and a notification is sent to the terminal to suspend all further operation. The state of the specified terminal is changed to blocked.

Step 1

To block a terminal, use the following example:

```
block session terminal=USR16;
```

Reply Example:

```
Reply : Success
```

Caution

If the terminal type of a terminal is associated with an external application such as SNMP, the external application is blocked as well.
Change Command

The `change` command changes the idle time of a session. The idle time defines the number of minutes that a user can be idle on a CLI or MAC interface before being automatically logged off the Cisco BTS 10200 Softswitch.

**Step 1**

To change the session idle time, use the following example:

```
change session idle-time=30;
```

Reply Example:
```
Reply : Success: Idle time set to 30 for new sessions.
```

Unblock Command

The `unblock` command is executed on a single terminal ID. The terminal is then unblocked and a notification is sent to the terminal for the user to resume normal operation. The state of the specified terminal is changed to `unblocked`.

**Step 1**

To unblock a single terminal, use the following example:

```
unblock session terminal=USR16;
```

Reply Example:
```
Reply : Success
```

Stop Command

The `stop` command is executed on a single terminal ID. The selected terminal is then notified to terminate and its associated terminal definition in the SMG is removed.

**Step 1**

To stop a specified terminal, use the following example:

```
stop session terminal=USR16;
```

Reply Example:
```
Reply : Success: Stop attempted on terminal <USR16>.
```
Provisioning the Call Agent, Subscribers, and Equal Access

This chapter describes initial Call Agent (CA), individual Subscriber, and Equal Access provisioning.

This chapter contains the following sections:
- Provisioning the Call Agent, page 5-1
- Provisioning an Individual Subscriber, page 5-3
- Provisioning Equal Access, page 5-4

Note

For detailed descriptions of each command, token, and available parameters, refer to the Cisco BTS 10200 Command Line Interface Reference Guide.

Provisioning the Call Agent

This section describes how to provision the Cisco BTS 10200 Softswitch Call Agent Office tables. The commands shown are typical, but may need to be adapted to your specific system. These steps are normally pre-provisioned with a script during installation.

Table 5-1 provides an overview of Call Agent provisioning.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Add the Call Agent (the Call Agent is provisioned first).</td>
</tr>
<tr>
<td>2.</td>
<td>Add the Call Agent profile.</td>
</tr>
<tr>
<td>3.</td>
<td>Add the Feature Servers.</td>
</tr>
<tr>
<td>4.</td>
<td>Add the Call Agent configuration.</td>
</tr>
<tr>
<td>5.</td>
<td>Add the office code.</td>
</tr>
<tr>
<td>6.</td>
<td>Add the point of presence.</td>
</tr>
<tr>
<td>7.</td>
<td>Add the media gateway profiles.</td>
</tr>
<tr>
<td>8.</td>
<td>Add the digit map.</td>
</tr>
</tbody>
</table>

To provision the Call Agent Office tables, perform the following steps:
Chapter 5  Provisioning the Call Agent, Subscribers, and Equal Access

Provisioning the Call Agent

Step 1  Add the Call Agent.
        add call-agent id=CA146; tsap-addr-sideA=190.10.100.200;

Step 2  Add the Call Agent profile.
        add call-agent-profile id=ca146; cms-supp=y; cms-id=12345; mgc-supp=y; mgc-id=12345;
        feid=financial-entity-id1; cdb-billing-supp=y; em-billing-supp=n; pri-rks-profile-id=rks1;
        sec-rks-profile-id=rks2;

Step 3  Add the Feature Servers.
        add feature-server id=FSPTC002; tsap-addr-sidea =190.101.100.103:11025; type=pots;

Step 4  Change the Call Agent configurations.
        change ca-config type=DEFAULT-POP; datatype=integer; value=255;
        change ca-config type=DEFAULT-office-service-id; datatype=integer; value=999;

Note  Repeat for each parameter. See Appendix B of the Cisco BTS 10200 Softswitch Command Line Interface Reference Guide for a complete list of provisionable parameters.

Step 5  Add the office codes.
        add office-code digit-string=972-213; office-code-index=1;

Step 6  Add the point-of-presence (POP).
        add pop id=1; state=TX; country=usa; timezone=CDT;

Step 7  Add the media gateway profile.
        add mgw-profile id=IAD2421; vendor=cisco;

Step 8  Add the digit map.
        add digit-map id=default;
        digit-pattern=0T|00|[(2-9)]11|[(2-9)xx][2-9]xxxxxx|1[(2-9)xx][2-9]xxxxxx|
        0[(2-9)xx][2-9]xxxxxx|01lxxxxxx.T|01xxxxxx.T|10lxxxxxx.W|x*xx|xxxxxxxxxxxxxxxxxxxxxxxxx;
Provisioning an Individual Subscriber

This section describes how to provision a Cisco BTS 10200 Softswitch individual subscriber. The
commands shown are typical, and must be adapted to your specific system. Table 5-2 provides an
overview of provisioning a subscriber.

Table 5-2 Overview of Subscriber Provisioning

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Add the destination.</td>
</tr>
<tr>
<td>2.</td>
<td>Add the dial plan profile.</td>
</tr>
<tr>
<td>3.</td>
<td>Add the dial plan.</td>
</tr>
<tr>
<td>4.</td>
<td>Add the media gateway profile.</td>
</tr>
<tr>
<td>5.</td>
<td>Add the media gateway.</td>
</tr>
<tr>
<td>6.</td>
<td>Add the terminations.</td>
</tr>
<tr>
<td>7.</td>
<td>Add the subscriber profile.</td>
</tr>
<tr>
<td>8.</td>
<td>Add the subscriber.</td>
</tr>
<tr>
<td>9.</td>
<td>Show the status of the media gateway.</td>
</tr>
<tr>
<td>10.</td>
<td>Control the media gateway in service.</td>
</tr>
<tr>
<td>11.</td>
<td>Show the status of the subscriber termination.</td>
</tr>
<tr>
<td>12.</td>
<td>Control the subscriber termination on a gateway.</td>
</tr>
</tbody>
</table>

To provision the Subscriber tables, perform the following steps:

**Step 1**
Add the destination.

```
add destination dest-id=local_call; call-type=local; route-type=sub;
```

**Step 2**
Add the dial plan profile.

```
add dial-plan-profile id=dp1; description= All subscribers in Dallas area with 972 prefix;
```

**Step 3**
Add the dial plan.

```
add dial-plan id=dp1; digit-string=972-213; reqd-digits=10; dest-id=local_call;
```

**Step 4**
Add the media gateway profile if you have not done so already when provisioning the CA.

```
add mgw-profile id=c2421.192;
```

**Step 5**
Add the media gateway.

```
add mgw id=c2421.192; tsap-addr=190.101.10.192; mgw-profile-id=IAD2421; rgw=y; call-agent id=CA101;
```

**Step 6**
Add the terminations.

```
add termination prefix=aaln/S1; mgw-id=c2421.192; port-start=1; port-end=16; type=line;
mgcp-pkg-type=line-mgcp;
```

**Step 7**
Add the subscriber profile.

```
add subscriber-profile id=individual; dial-plan-id=dp1; pop-id=1
```
Provisioning Equal Access

This section describes how to set up a subscriber and the Cisco BTS 10200 Softswitch for equal access dialing based on an interexchange carrier (IXC) Preferred intraLATA carrier (PIC). This procedure applies to direct distance dialing (DDD) and international direct distance dialing (IDDD) dialing and dial plans. This procedure can also be applied to local service provider equal access using the PIC2 field in the Cisco BTS 10200 Softswitch Subscriber table.

Note

Ensure that all residential gateways, trunking gateways, and all other translations support the commands described in this section.

For general carrier and U.S. domestic dialing information, see the following URL:
http://www.nanpa.com

Table 5-3 provides an overview of provisioning equal access.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Add the carrier ID.</td>
</tr>
<tr>
<td>2.</td>
<td>Change the PIC1 to the appropriate interLATA and international carrier PIC.</td>
</tr>
<tr>
<td>3.</td>
<td>Add an interLATA dummy route.</td>
</tr>
<tr>
<td>4.</td>
<td>Add a route guide ID.</td>
</tr>
<tr>
<td>5.</td>
<td>Add a destination for interLATA calls.</td>
</tr>
<tr>
<td>6.</td>
<td>Add dial plan entries for all U.S. supported NPAs.</td>
</tr>
<tr>
<td>7.</td>
<td>Add an international dummy route.</td>
</tr>
<tr>
<td>8.</td>
<td>Add the international route guide ID.</td>
</tr>
</tbody>
</table>
To set up equal access dialing, perform the following steps:

**Step 1**  Add the carrier ID. This sets the carrier up and puts it in-service.

```
add carrier id=0288; status=ins; inter=y; intra=y; intl=y; casual=y; cut-thru=y;
  op-services=y; send-cn=n; send-csp=y; use-dial-plan=n;
```

**Step 2**  Change the PIC1 to the appropriate interLATA and international carrier PIC. This presubscribes a subscriber to a carrier so the subscriber does not have to dial 101+4 digit carrier code + the number to make a call.

```
change subscriber; id=motfb4/1; name=John Doe; PIC1=0288; PIC2=NONE; PIC3=NONE;
```

**Step 3**  Add an interLATA dummy route. This is required to set up a dial plan.

```
add route id=EA-IXC;lcr=n; tgn1-id=null;
```

**Step 4**  Add a route guide ID. This is required to set up a dial plan.

```
add route-guide id=EA-IXC; policy-type=route; policy-id=EA-IXC;
```

**Step 5**  Add a destination for interLATA calls. This is required to set up a dial plan.

```
add destination dest-id=Interlata-IXC; call-type=InterLata; route-type=route;
  route-guide-id=EA-IXC;
```

**Step 6**  Add dial plan entries for all U.S. supported Numbering Plan Areas (NPAs). This allows verification that a subscriber can call a particular NPA.

```
add dial-plan id=dp-mot; digit-string=201; reqd-digits=10; dest-id=Interlata-IXC
```

**Step 7**  Add an international dummy route. This is required to set up an international dial plan.

```
add route id=INTL-IXC; lcr=n; tgn1-id=null
```

**Step 8**  Add the international route guide ID. This is required to set up an international dial plan.

```
add route-guide id=INTL-IXC; policy-type=route; policy-id=INTL-IXC;
```

**Step 9**  Add the international destination. This is required to set up an international dial plan.

```
add destination dest-id=INTL-IXC; call-type=INTL; route-type=route;
  route-guide-id=INTL-IXC;
```

**Step 10**  Add international dial plans for all supported country codes. This allows verification that a subscriber can call a particular country.

---

**Table 5-3  Overview of Provisioning Equal Access (continued)**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.</td>
<td>Add the international destination.</td>
</tr>
<tr>
<td>10.</td>
<td>Add international dial plans for all supported country codes.</td>
</tr>
<tr>
<td>11.</td>
<td>Add the SS7 Feature Group D (FGD) equal access trunk group to the IXC switch.</td>
</tr>
<tr>
<td>12.</td>
<td>Add the SS7 trunks to the IXC switch.</td>
</tr>
<tr>
<td>13.</td>
<td>Control the trunk termination in service.</td>
</tr>
<tr>
<td>14.</td>
<td>Add the route to the IXC switch.</td>
</tr>
<tr>
<td>15.</td>
<td>Add the route guide ID to the IXC switch.</td>
</tr>
<tr>
<td>16.</td>
<td>Add the route guide ID to the Carrier table.</td>
</tr>
<tr>
<td>17.</td>
<td>Add the circuit code if the TNS parameter is required.</td>
</tr>
</tbody>
</table>
Provisioning Equal Access

add int1-dial-plan id=RTP01; cc=34; min-digits=6; max-digits=16; dest-id=INTL-IXC

Step 11 Add the SS7 Feature Group D (FGD) equal access trunk group to the IXC switch. This builds a trunk to the next service provider.

add ss7-tg-profile id=IXC-FGD; type=A7; cot-orig=y; cot-freq=10; T-IAM=20;
add trunk-grp id=205; call-agent-id=CA146; tg-type=ss7;
dpc=214-110-205; traffic-type=tandem;
select-policy=DSC; glare=all; tg-profile-id=IXC-FGD; dial-plan-id=Incoming; No-answer-tmr=240; CLI=RLGHIXC;

Note Refer to GR-394 for SS7 parameters that must be sent in SS7 messages through the FGD interface.

Step 12 Add the SS7 trunks to the IXC switch. This sets up the actual bearer channel.

add trunk cic-start=1; cic-end=24; tgn-id=205; mgw-id=C0201_VISM5;
termination-prefix=vism/t1-1/; termination-port-start=1; termination-port-end=24;
equip trunk-termination tgn-id=205; cic=1-48;

Step 13 Control the trunk termination in service.

control trunk-termination tgn-id=205; cic=1-48; mode=INS;

Step 14 Add the route to the IXC switch. This provides the path to the service provider providing equal access.

add route id=SS7-IXC; lcr=N; tgn1-id=205;

Step 15 Add the route guide ID to the IXC switch. This is required to route to a service provider.

add route-guide id=SS7-IXC; policy-type=route; policy-id=SS7-IXC;

Step 16 Add the route guide ID to the Carrier table. This provides the path to route directly to a service provider.

change carrier id=0288; status=ins; inter=y; intra=y; intl=y; casual=y; cut-thru=y;
op-services=y; send-cn=y; send-csp=y; use-dial-plan=n; route-guide-id=SS7-IXC;

Note These are typical values for most ICXs. The values can differ based on the IXC carrier.

Step 17 Add the circuit code if the transit network selection (TNS) parameter is required.

add circuit-code tgn-id=205; nat-cc=9; opr-cc=14; nat-opr-cc=14; sac-cc=9; da-cc=9;

Note The Circuit Code table is used only when there are special requirements. The values given can differ based on the IXC carrier. The Cisco BTS 10200 Softswitch default values work for most ICXs.
Provisioning Features and Services

This chapter describes how to provision the features and services supported by the Cisco BTS 10200 Softswitch.

Refer to the *Cisco BTS 10200 Softswitch System Description* for feature activation and deactivation steps.

This chapter uses the following conventions:

- **Basic feature and service provisioning**—Identifies provisioning that is done per subscriber, multi line hunt group (MLHG), Centrex, or only once during initial Cisco BTS 10200 Softswitch configuration. Provisioning at initial configuration is normally not repeated.
- **Prerequisites**—Identifies any prerequisite provisioning or other tasks that must be accomplished before provisioning a specific feature or service.
- **Supported interfaces**—Identifies the interfaces specific to the feature or service.

Features can be assigned to any fname token, that is, to fname1, fname2 and so forth.

This chapter makes the following assumptions:

- **Basic resource provisioning** has already been done. This includes provisioning of Call Agents, Feature Servers, media gateways, trunks, terminations.
- **Basic calling** has been provisioned and works for a subscriber.
- **All command-line interface (CLI) command examples** are for illustration purposes only and represent the mandatory provisioning tokens specific to a feature. Using just the mandatory tokens may not be sufficient to provide service.
- For default values, usage rules, and token definitions, refer to the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

In this chapter, whenever the `add` command is used, if the table has already been added, use the `change` command instead.
800 Local Dialed Number Identification Service

The 800 Local Dialed Number Identification Service (DNIS) is used in call center applications. DNIS provides (outpulses) the original dialed 800 number and/or automatic number identification (ANI) information to the call center.

Prerequisites

None.

Supported Interfaces

SS7

Provisioning 800 Local DNIS

To provision 800 local DNIS, perform the following steps:

Step 1 Add the policy nxx ID.
add policy-nxx id=88888; route=carrier-0220;

Step 2 Add the route guide ID.
add route-guide id=99999; policy-type=nxx; policy-id=88888;

Step 3 Add the customer group ID.
add cust-grp id=ip1; overflow-carrier=8888; ani-wb-list=black; II-restrict-list=black; dnis-pattern=IIAAAAAAAAAA*8001234567*; route-guide-id=99999;

Step 4 Add the DN2 customer group digit string.
add dn2cust-grp digit-string=800-306-4321; translated-dn=306-603-4321; cust-grp-id=ip1;

Step 5 Change the customer group ID.
change cust-grp id=ip1; dnis-pattern=*II#IIIIIIIIIIIIIIII#22456785*;
change cust-grp id=ip1; dnis-pattern=*II*IIIIIIIIIIIIIIII*123456789088898*;

where:

• II = the information digit (originating line information (OLI))
• AAAAAAAAA = the calling party
• 22456785 = the called party
800 Local Time of Day and Day of Week

The 800 Local Time of Day (TOD) and Day of Week (DOW) feature is route based according to the time of day and day of week.

Prerequisites

None.

Supported Interfaces

SS7, MGCP, ISDN

Provisioning 800 Local TOD and DOW

To provision 800 local TOD and DOW, perform the following steps:

Step 1  Add the policy nxx ID.
add policy-nxx id=201; translated-dn=972-518-1001;
add policy-nxx id=202; translated-dn=972-518-1002;
add policy-nxx id=203; translated-dn=972-518-1003;

Step 2  Add the policy time of day ID.
add policy-tod id=TOD101; doy1=09-06; doy1-policy-type=nxx; doy1-policy-id=201;
start-dow1=MON; stop-dow1=FRI; start-time1=07:00; stop-time1=17:00; policy-type1=nxx;
policy-id1=202; default-policy-type=nxx; default-policy-id=203;

Step 3  Add the policy origin dependent routing (ODR) ID.
add policy-odr id=ODR1; digit-string=972; policy-type=TOD; policy-id=TOD101;

Step 4  Add the route guide ID.
add route-guide id=800-234-3000; policy-type=ODR; policy-id=ODR1;

Step 5  Add the customer group ID.
add cust-grp id=500; route-guide-id=800-234-3000;

Step 6  Add the DN2 customer group information.
add dn2cust-grp digit-string=800-654-3210; cust-grp-id=500;

Examples:
1. When a called number is 800-654-3210 and the day is today’s date, the call is translated to 972-518-1001.
2. When a called number is 800-654-3210 and the day is not today’s date, but the day is Monday through Friday and the time is between 7:00 a.m. to 5:00 p.m., the call is translated to 972-518-1002.
800 Policy Point of Presence Routing

The 800 Policy Point of Presence (POP) routing feature is the route in which an 800 call takes when a long distance carrier interfaces with a local telephone company.

Prerequisites

The following steps are required before you can provision an 800 policy POP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Add the global title and sub system information into the Omni file, where the global title translation (GTT) = 8, and subsystem = 247.</td>
</tr>
</tbody>
</table>

LNP: CREATE-GT:TT=11,NP=ISDN-TEL,DIG="514606",PC=1-101-0,SSN=247,RI=DEF;  
IN-800: CREATE-GT:TT=254,NP=ISDN-TEL,DIG="877",PC=1-101-0,SSN=254,RI=DEF;  
CNAM: CREATE-GT:TT=5,NP=ISDN-TEL,DIG="408256",PC=1-101-0,SSN=232,RI=DEF;  

Where:
- CREATE-GT—command  
- TT—translation type  
- NP—numbering plan  
- DIG—digits  
- PC—destination point code  
- SSN—subsystem number  
- RI—Routing indicator.

Supported Interfaces

MGCP, ISDN, SS7

Provisioning an 800 Policy POP

To provision routing for an 800 policy POP, perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Add the POP ID.  
  add pop id=21; state=tx;  
| 2    | Add the carrier ID.  
  add carrier id=0288; status=ins;  
| 3    | Add the policy POP ID.  
  add policy-pop id=POP20; pop-id=21; policy-type=route;policy-id=ss7-1  
| 4    | Add the route guide ID.  
  add route-guide id=pop20-rg; policy-type=pop;policy-id=POP20;  

Anonymous Call Rejection

The Anonymous Call Rejection (ACR) feature allows subscribers to reject calls from parties that have set their privacy feature to prevent calling number delivery. When ACR is active, the called party is not alerted of incoming calls that are rejected. The incoming call is rerouted to a denial announcement indicating that private numbers are not accepted by the called party.

To complete a call to the party with ACR, the calling party must enter the vertical service code (VSC) (*82-CIDSD) to activate calling identity delivery and then place a call to the party with ACR. Incoming calls to the called party with ACR are checked even if the called party is offhook.

Prerequisites

To complete a call to a party with ACR, the calling party must allow calling number delivery. The calling must also have the standard Core and Subscriber default provisioning.

Supported Interfaces

MGCP

Provisioning ACR

To provision ACR, perform the following steps:

Step 1  Add the feature activation name.

```
add feature FNAME=ACR_ACT;tdp1=COLLECTED_INFORMATION;td1=VERTICAL_SERVICE_CODE;
ttype1=R;feature-server-id=FSPTC235;description=ACR Activation;grp-feature=n;
```

Step 2  Add the feature deactivation name.

```
add feature FNAME=ACR_DEACT;tdp1=COLLECTED_INFORMATION;td1=VERTICAL_SERVICE_CODE;
ttype1=R;feature-server-id=FSPTC235;description=ACR Deactivation;
```
Step 3  Add the feature invocation name

```
add feature
fname=ACR;tdp1=TERMINATION_ATTEMPT_AUTHORIZED;tid1=TERMINATION_ATTEMPT_AUTHORIZED;
ttype1=R;feature-server-id=FSPTC235;description=ACR Deactivation;
```

Step 4  Add the VSC digit string.

```
add vsc digit-string=*87;fname=ACR_DEACT
add vsc digit-string=*77;fname=ACR_ACT
```

Step 5  Create a service with the ACR, ACR_ACT, ACR_DEACT

```
add service id=20; fname1=ACR; fname2=ACR_ACT; fname3=ACR_DEACT;
```

Step 6  Assign the service to the subscriber

```
add sub-service-profile sub-id=sub1-ctx; service-id=20;
```

---

**Provisioning ACR for a Centrex Group**

To provision ACR for a Centrex group, perform the following steps:

Step 1  Show the Centrex group and note what customer dial plan (CDP) the main-sub-id is in. Use this CDP for Step 2.

```
show ctxg
```

Step 2  Add the CDP ID.

```
add cdp ID=cdp1; digit-string=*77; nod=vsc; fname=ACR_ACT;
cat-string=1111111111111111111111;
add cdp ID=cdp1; digit-string=*87; nod=vsc; fname=ACR_DEACT;
cat-string=1111111111111111111111;
```

Step 3  Assign the feature to the subscriber.

```
add sub-service-profile sub-id=sub1-ctx; service-id=20;
```

---

**Automatic Callback**

The Automatic Callback (AC) feature allows subscribers to set up a call to the last party that they called without having to redial the telephone number. If the called party is busy, the subscriber can hang up. Then when the called party becomes idle the call is automatically connected. AC can be provided to Office, Centrex, and MLHG subscribers

**Prerequisites**

None.
Supported Interfaces

MGCP

Provisioning AC

To provision AC, perform the following steps:

**Step 1** Change the Call Agent ID.

```plaintext
change call-agent id=CA166;tsap-addr-sidea=sim-SYS01CA.ipclab.cisco.com:9146;
```

*Note* The port=9146 must match the service interaction manager (SIM) port of the Call Agent platform.cfg file.

**Step 2** Change the Feature Server ID.

```plaintext
change feature-server id=FSPTC235;type=pots;
tsap-addr-sidea=pots-SYS01PTC.ipclab.cisco.com:11235
```

*Note* The port=11235 must match the port in the FSPTCnnn platform.cfg file.

**Step 3** Add the activation and deactivation feature names.

```plaintext
add feature fname=AC_ACT; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE;
ttype1=R; description=Automatic Callback Activation; feature-server-id=FSPTC235;
add feature fname=AC_DEACT; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE;
ttype1=R; description=Automatic Callback Deactivation; feature-server-id=FSPTC235;
add feature fname=AC; fname1=AC_ACT; fname2=AC_DEACT; feature-server-id=FSPTC235;
```

**Step 4** Add the VSC digit string.

```plaintext
add vsc digit-string=*66; fname=AC_ACT;
add vsc digit-string=*86; fname=AC_DEACT;
```

**Step 5** Add the feature to the service ID.

```plaintext
add service id=41; fname=AC;
```

**Step 6** Assign the service to the subscriber.

```plaintext
add subscriber-service-profile sub-id=ubr41@cisco.com;service-id=41
```

*Note* You must change the npa-nxx field of the office-code digit-string of the called and calling DNs as follows: *change office-code. digit-string=512-234; call-agent-id=CA166;*
Provisioning AC for a Centrex Group

To provision AC for a Centrex group, perform the following steps:

**Step 1**  
Show the Centrex group and note what customer dial plan (CDP) the main-sub-id is in. Use this CDP for Step 2.

```
show ctxg
```

**Step 2**  
Add the CDP ID.

```
add cdp ID=cdp1; digit-string=*66; nod=vsc; fname=AC_ACT;
cat-string=111111111111111111111;
add cdp ID=cdp1; digit-string=*86; nod=vsc; fname=AC_DEACT;
cat-string=111111111111111111111;
```

**Step 3**  
Add the VSC digit string.

```
add vsc digit-string=*66; fname=AC_ACT;
add vsc digit-string=*86; fname=AC_DEACT;
```

**Step 4**  
Add the feature to the service ID.

```
add service id=41; fname1=AC;
```

**Step 5**  
Assign the service to the subscriber.

```
add sub-service-profile sub-id=sub1-ctx; service-id=41;
```

Automatic Number Identification Screening

The Automatic Number Identification (ANI) Screening feature is call screening based on the calling party number for trunk groups.

**Prerequisites**

None.

**Supported Interfaces**

SS7, ISDN
Provisioning ANI Screening

To provision ANI screening, perform the following steps:

**Step 1**
Add the feature name.

```
add feature fname=COS; tdp1=COLLECTED_INFORMATION; tid1=cos-trigger; ttype1=R;
description=Class of service screening; feature-server-id=FSPTC235;
```

**Step 2**
Add the service ID.

```
add service id=21; fname1=COS;
```

**Step 3**
Add the class of service ID.

```
add cos-restrict id=SS7-LOCAL; national-restrict-type=NATIONAL-ONLY;
intl-restrict-type=NO-CC-ALLOWED; national-wb-list=BLACK; block-900=Y; block-976=Y;
block-da=Y; block-nanp-oper-assist=Y; block-intl-oper-assist=Y;
```

**Step 4**
Add the trunk group feature data.

```
add trunk-grp-feature-data tgn-id=3;
cos-restrict-id=SS7-LOCAL1;tg=ss7-trunk-1;casual-call=y;
```

**Step 5**
Add the trunk group service profile.

```
add trunk-grp-service-profile tgn-id=3; service-id=21;
priority=1;tg=ss7-trunk-1;casual-call=y;
```

**Note**
The is for an incoming SS7 on tgn- id=3

**Step 6**
Add the ANI ID.

```
add ani id=972-519-2000; ACTIVE=N;
```

**Note**
If active=n, the ANI cannot make a call.

To activate ANI screening, set active=y, as follows:

```
add ani id=972-519-2000; ACTIVE=Y;
```
Automatic Recall

The Automatic Recall (AR) feature is an incoming call management feature that allows a subscriber to automatically set up a call to the last incoming number. If the called party is busy, the subscriber can hang up, activate AR, and then when the called party becomes idle, the call is automatically connected. This section includes provisioning AR and provisioning AR for a Centrex group.

Prerequisites

None.

Supported Interfaces

MGCP

Provisioning AR

To provision AR, perform the following steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Change the Call Agent ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>change call-agent id=CA166;tsap-addr-sidea=sim-SYS01CA.ipclab.cisco.com:9146;</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>The port=9146 must match the SIM port in CAnnn platform.cfg file.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Change the Feature Server ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>change feature-server id=FSPTC235;type=pots;TSAP-ADDR-SIDEA=pots-SYS01PTC.ipclab.cisco.com:11235</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>The port=11235 must match the port in FSPTCnnn platform.cfg file.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Add the activation and deactivation feature names.</th>
</tr>
</thead>
<tbody>
<tr>
<td>add feature fname=AR_ACT; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R; description=Automatic Callback Activation; feature-server-id=FSPTC235;</td>
<td></td>
</tr>
<tr>
<td>add feature fname=AR_DEACT; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R; description=Automatic Callback Deactivation; feature-server-id=FSPTC235;</td>
<td></td>
</tr>
<tr>
<td>add feature fname=AR; fname1=AR_ACT; fname2=AR_DEACT; feature-server-id=FSPTC235;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Add the VSC digit string.</th>
</tr>
</thead>
<tbody>
<tr>
<td>add vsc digit-string=*69; fname=AR_ACT;</td>
<td></td>
</tr>
<tr>
<td>add vsc digit-string=*89; fname=AR_DEACT;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Add the service ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>add service id=42; fname=AR;</td>
<td></td>
</tr>
</tbody>
</table>
Step 6  Assign the service to the subscriber.

```
add subscriber-service-profile sub-id=ubr41@cisco.com; service-id=42
```

**Note**  You must change the npa-nxx of the office-code digit-string of the called and calling DNs as follows: `change office-code digit-string=512-234; call-agent-id=CA166;`

---

**Provisioning AR for a Centrex Group**

To provision AR for a Centrex group, perform the following steps:

**Step 1**  Show the Centrex group ID.

```
show ctxg
```

Note what CDP the token main-sub-id is in.

**Step 2**  Add the CDP ID.

```
add cdp ID=cdp1; digit-string=*69; nod=vsc; fname=AR_ACT; cat-string=1111111111111111;
add cdp ID=cdp1; digit-string=*89; nod=vsc; fname=AR_DEACT; cat-string=1111111111111111;
```

**Step 3**  Create a service with the feature AR.

```
add service id=42; fname1=AR;
```

**Step 4**  Assign the service to the subscriber.

```
add sub-service-profile sub-id=sub1-ctx; service-id=42;
```

---

**Busy Line Verification and Busy Line Interrupt**

The Busy Line Verification (BLV) service allows a subscriber to obtain operator assistance to determine if a called line is in use. BLV is an Office-based feature. The preset default service ID is 999. This value is provisionable in the databases. For example:

```
show service id=999;
```

Reply Example:

```
Reply : 1 entry found.

ID=999
FNAME1=8XX
FNAME2=LNP
FNAME3=USTWC
FNAME4=CHD
FNAME5=911
FNAME7=BLV
```
The Busy Line Interrupt (BLI) service allows the operator to interrupt the called party’s line and relay a message. If the interrupted party hangs up, the subscriber can originate a new call, providing BLI is not prohibited in advance by the interrupted party. Also, at the subscriber’s request, the operator can connect the subscriber directly to the called line.

**Prerequisites**

For the BLV barge-in feature to work, the channel-associated signaling (CAS) trunk quality of service (QoS) and subscriber QoS must match.

**Supported Interfaces**

The BLV Operator origination is CAS MF WINK-START.

The BLV terminations are MGCP subscribers.

**Provisioning Office BLV**

To provision office BLV, perform the following steps:

**Step 1**

Add the default office service ID.

```
change ca-config default-office-service-id=999;
```

**Step 2**

Add the BLV service to the default office service.

```
change service id=999; fname=BLV;
```

**Step 3**

Provision the feature in the office.

```
add feature fname=BLV; tdp1=termination-attempt; tid1=BLV; ttype1=R;
feature-server-id=fsptc235; description=Busy-line verification; grp-feature=N;
```

**Step 4**

Set the BLV CAS trunk group profile as type *no-test*.

```
add cas-tg-profile id=cas-blv; no-test-trunk=y;
```

**Step 5**

Set the MGCP package type associated with CAS trunk termination to type MO.

```
add termination id=S0/DS1-1/1; mgw-id=c2421.1001; mgcp-package-type=MO;
```

**Step 6**

Set the quality of service parameter of the trunk group.

```
add trunk-grp id=152; qos-id=pcm;
```
Provisioning BLV for Subscribers, Centrex, and MLHG

To provision BLV for a subscriber, Centrex, and multiline hunt group (MLHG), perform the following steps:

**Step 1** Add the channel-associated signaling (CAS) trunk group profile ID.
```
add cas-tg-profile id=cas-blv; TYPE=MF-WINKSTART; OSS-SIG=N; TEST-LINE=N; NO-TEST-TRUNK=Y; E911=N;
```

*Note* Ensure that no-test-trunk = Y.

**Step 2** Add the trunk group ID.
```
add trunk-grp id=4007; tg-type=CAS; dial-plan-id=dp1; sel-policy=LRU; direction=BOTH; glare=ODD; tg-profile-id=cas-blv; call-agent-id=CA166; status=oos;
```

**Step 3** Add the termination prefix. This example adds S2/DS1-1/.
```
add termination prefix=S2/DS1-1/; mgw-id=10.89.227.158; type=TRUNK; mgcp-pkg-type=MT; port-start=1; port-end=8;
```

**Step 4** Add the trunk.
```
add trunk cic-start=1; cic-end=8; tgn-id=4007; termination-prefix=S2/DS1-1/; mgw-id=10.89.227.158; termination-port-start=1; termination-port-end=8;
```

**Step 5** Set the quality of service parameter for the specific subscriber.
```
add sub-profile id=sp-cas-blv; Digit-map-id=default; dial-plan-id=dp1; local-pfx1-opt=nr; toll-pfx1-opt=rq; pop-id=1; oli=0; ea-use-pic1=y;
```

**Step 6** Set access permissions for line verification on the subscriber line. This example denies Office permission for line verification on a line.
```
add subscriber-feature-data sub-id=plano-sub1; fname=BLV; type1=DENIED
```

**Step 7** Add the subscriber ID.
```
add sub id=cas-blv-mf-wk-4007; category=PBX; name=cas4007; status=ACTIVE; email=cas4007@ipclab.cisco.com; language=english; type-of-service=00; sip-url=sip-url; billing-dn=972-619-4007; dn1=972-619-4007; privacy=none; ring-type-dn1=1; tgn-id=4007; pic1=3333; pic2=2222; pic3=9999; grp=n; usage-sens=n; sub-profile-id=sp-cas-blv;
```

**Step 8** Add the route ID.
```
add route id=cas4007; lcr=y; tgn1-id=4007; del-digits1=0; del-digits2=0; del-digits3=0; del-digits4=0; del-digits5=0; del-digits6=0; del-digits7=0; del-digits8=0; del-digits9=0; del-digits10=0;
```

**Step 9** Add the route guide ID.
```
add route-guide id=cas4007; policy-type=ROUTE; policy-id=cas4007;
```
Call Admission Control Using the Resource Reservation Protocol

This feature provides static value for media gateway support of the Resource Reservation Protocol (RSVP). RSVP field is used only if the Call Agent cannot read dynamic RSVP support data from a media gateway. This ensures enough bandwidth reserves for IP packets.

The gateways can be instructed to perform a reservation using RSVP on a given connection. When a reservation is needed, the call agent specifies the reservation profile to be used, which is either “controlled load” or “guaranteed service.” The absence of a reservation can be indicated by asking for the “best effort” service, which is the default value of this parameter.

Prerequisites

In the Media Gateway Profile table, the field rsvp-unsupp=n.

Supported Interfaces

Not applicable

Provisioning Call Admission Control

To provision Call Admission Control using RSVP, perform the following steps:

Step 1
Add the quality of service ID.

```
add qos id=RSVP_PCMU; codec-type=G711U; rsvp-required=Y; resource-reservation=G;
```

Step 2
Assign the quality of service ID to the subscriber.

```
change sub id=sub1; qos-id=RSVP_PCMU;
```

Call Block

The Call Block feature allows a subscriber to block incoming calls from the directory number (DN) of the last received call. For the Call Block feature to work, a subscriber must be subscribed to the Selective Call Reject (SCR) feature. Once call block is activated against a specified DN, that DN remains in the subscriber’s SCR list. A subscriber can use this feature to block callers (such as telemarketers) where the caller’s DN is not known. Call block can be provided to Office, Centrex, and MLHG subscribers.

Prerequisites

None.
Supported Interfaces

Not applicable

Provisioning Office Call Block

To provision office call block, perform the following steps:

Step 1  Add the Call Block feature.

```
add feature FNAME=CBLK; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R;
feature-server-id=FSPTC235; description=Call Block - Reject Caller; grp-feature=N;
```

Step 2  Add the VSC code in the VSC table.

```
add vsc; digit-string=*97; FNAME=CBLK;
```

Provisioning Call Block for a Subscriber

To provision call block for a subscriber, perform the following steps.

Note This feature works in conjunction with the SCR feature. Therefore, for the call to be rejected by call block, SCR must be assigned to the subscriber and activated. See the “Screen List Editing” section on page 6-63 for directions for provisioning SCR.

Step 1  Add a service with the Call Block feature.

```
add service; id=1; fname1=CBLK;
```

Step 2  Assign the service to the subscriber.

```
add subscriber-service-profile; sub-id=sub1; service-id=1;
```

Note If the subscriber does not exist, use the add command.

Provisioning Call Block for Centrex Subscribers

To provision call block for Centrex subscribers, perform the following step:

Step 1  Add the custom dial plan (CDP) ID.

```
change cdp; id=cdp1; digit-string=*97; nod=VSC; FNAME=CBLK; cat-string=111111111111111;
```
Provisioning Call Block for MHLG Subscribers

MLHG provisioning is the same as provisioning call block for a subscriber.

Call Forwarding Busy

The Call Forwarding Busy (CFB) feature allows subscribers to forward incoming calls to another number when they are already on a call. Call block can be provided to Office and Centrex subscribers.

Prerequisites

None.

Supported Interfaces

Not applicable

Provisioning CFB

To provision CFB, perform the following steps:

Step 1

Add the activation and deactivation feature names.

```bash
add feature fname=CFBVA;tdp1=COLLECTED_INFORMATION;tid1=VERTICAL_SERVICE_CODE;ttype1=R;
feature-server-id=FSPTC235;description=Call Forwarding Busy Activation;grp-feature=N;

add feature fname=CFBVD;tdp1=COLLECTED_INFORMATION;tid1=VERTICAL_SERVICE_CODE;ttype1=R;
feature-server-id=FSPTC235;description=Call Forwarding Busy Deactivation;grp-feature=N;

add feature fname=CFBI;tdp1=COLLECTED_INFORMATION;tid1=VERTICAL_SERVICE_CODE;ttype1=R;
feature-server-id=FSPTC325;type1=intl;value1=n;description=CFB Interrogation;grp-feature=N;

add feature fname=CFB;tdp1=t-busy;tid1=t-busy;ttype1=R;fname1=CFBVA;fname2=CFBVD;
fname3=CFBI;feature-server-id=FSPTC235;description=Call Forwarding Busy;grp-feature=N;
```

Step 2

Add the VSC codes.

```bash
add vsc digit-string=*90;FNAME=CFBVA;
add vsc digit-string=*91;FNAME=CFBVD;
add vsc digit-string=*96;FNAME=CFBI;
add vsc digit-string=1190;FNAME=CFBVA;
add vsc digit-string=1191;FNAME=CFBVD;
add vsc digit-string=1196;FNAME=CFBI;
```

Note

If the subscriber has call waiting activated with CFB, the subscriber hears a call waiting tone if another party calls instead of the call being forwarded. However, if another party calls at the same time, the call is forwarded because call waiting is active and the CFB activated subscriber is busy.
Step 3  Add the service.
        add service id=545; fname=CFB;

Step 4  Assign the service to the subscriber.
        add subscriber-service-profile sub-id=ubr@cisco.com; service-id=545;

Provisioning CFB for Centrex Subscribers

To provision CFB for Centrex subscribers, perform the following steps:

Step 1  Add the feature into the Custom Dial Plan table for the Centrex group.
        add custom-dial-plan
            id=cdp1; digit-string=*90; nod=vsc; fname=CFBVA; cat-string=1111111111111111;
        add custom-dial-plan
            id=cdp1; digit-string=*91; nod=vsc; fname=CFBVOD; cat-string=1111111111111111;
        add custom-dial-plan
            id=cdp1; digit-string=*96; nod=vsc; fname=CFBII; cat-string=1111111111111111;

Call Forwarding No Answer

The Call Forwarding No Answer (CFNA) feature allows a subscriber to instruct the network to forward calls when there is no answer on the subscriber’s phone. A typical forwarding address is voice mail. The subscriber can activate and deactivate this feature through the dual tone multifrequency (DTMF) interface on the handset. Once the feature is activated, the feature remains active until the subscriber deactivates it. When the feature is activated, any incoming calls attempted to the subscriber’s phone that are not answered in the first six rings are forwarded to the specified number.

When provisioning CFNA, TO in the Feature table specifies the time out for reporting No-Answer. This TO can be changed to N seconds using the following command:

change feature; fname=CFNA; type1=TO; value1=N;

Use the following command to activate the feature or change the forwarding-dn for a subscriber sub-1:

add sub-feature-data; sub-id=sub-1; active=y; fname=CFNA; type1=fdn1; value1=9723311261;

Prerequisites

None.

Supported Interfaces

Not applicable
Provisioning CFNA

To provision CFNA, perform the following steps:

Step 1  Add the activation and deactivation feature names.

```plaintext
add feature fname=CFNAVA;tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R;
feature-server-id=FSPTC235; description=Call Forwarding No Answer Activation;
grp-feature=n;

add feature fname=CFNAVD;tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R;
feature-server-id=FSPTC235; description=Call Forwarding No Answer deactivation;
grp-feature=n;

add feature fname=CFNAI;tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R;
feature-server-id=FSPTC235; description=Call Forwarding No Answer interrogation;
grp-feature=n;

add feature fname=CFNA; tdp1=call-accepted; tid1=call-accepted; ttype1=R; fname1=CFNAVA;
fname2=CFNAVD; fname3=CFNAI; feature-server-id=FSPTC235; type1=TO; value1=30;
description=Call Forwarding No Answer to=timeout; grp-feature=n;
```

Step 2  Add the VSCs.

```plaintext
add vsc digit-string=*92;FNAME1=CFNAVA;
add vsc digit-string=*93;FNAME2=CFNAVD;
add vsc digit-string=*97;FNAME3=CFNAI;
add vsc digit-string=1192;FNAME=CFNAVA;
add vsc digit-string=1193;FNAME=CFNAVD;
add vsc digit-string=1197;FNAME=CFNAI;
```

Step 3  Add the service.

```plaintext
add service id=546; fname1=CFNA;
```

Step 4  Assign the service to the subscriber.

```plaintext
add subscriber-service-profile sub-id=ubr@cisco.com; service-id=546;
```

Provisioning CFNA for Centrex Subscribers

To provision CFNA for Centrex subscribers, perform the following steps:

Step 1  Add the feature into the Custom Dial Plan table for the Centrex group.

```plaintext
add custom-dial-plan
id=cdp1;digit-string=*92;nod=vsc;fname=CFNAVA;cat-string=111111111111111111;

add custom-dial-plan id=cdp1;digit-string=*93;
nod=vsc;fname=CFNAVD;cat-string=111111111111111111;

add custom-dial-plan id=cdp1;digit-string=*97;
nod=vsc;fname=CFNAI;cat-string=111111111111111111;
```
Call Forwarding Unconditional

The Call Forwarding Unconditional (CFU) feature allows a subscriber to forward all incoming calls to another telephone number until the feature is explicitly deactivated. When CFU is activated on the telephone line, the subscriber hears only a short reminder ring at the number, after which the forwarded telephone line is offered the call.

Prerequisites

None.

Supported Interfaces

Not applicable

Provisioning CFU

To provision CFU, perform the following steps:

**Step 1** Add the feature names.

```
add feature fname=CFUA; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R; feature-server-id=FSPTC235; description=Call Forwarding Unconditional Activation; grp-feature=N;
```

```
add feature fname=CFUD; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R; feature-server-id=FSPTC235; description=Call Forwarding Unconditional deactivation; grp-feature=N;
```

```
add feature fname=CFUI; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R; feature-server-id=FSPTC235; description=Call Forwarding Unconditional interrogation; grp-feature=N;
```

```
add feature fname=CFU; tdp1=TERMINATION_ATTEMPT_AUTHORIZED; tid1=TERMINATION_ATTEMPT_AUTHORIZED; ttype1=R; fname1=CFUA; fname2=CFUD; fname3=CFUI; feature-server-id=FSPTC235; description=CFU MCF=multiple call forwarding allowed, rr=ring reminder; grp-feature=N;
```

**Step 2** Add the VSC codes.

```
add vsc digit-string=*72; FNAME1=CFUA
add vsc digit-string=*73; FNAME2=CFUD
add vsc digit-string=*98; FNAME3=CFUI
add vsc digit-string=1172; FNAME=CFUA
add vsc digit-string=1173; FNAME=CFUD
add vsc digit-string=1198; FNAME=CFUI
```

**Step 3** Create a service with the CFU feature.

```
add service id=547; fname1=CFU;
```

**Step 4** Assign the service to the subscriber.

```
add subscriber-service-profile sub-id=ubr@cisco.com; service-id=547;
```
Provisioning CFU for Centrex Subscribers

To provision CFU for Centrex subscribers, perform the following steps:

**Step 1** Add the feature into the Custom Dial Plan table for the Centrex group.

```plaintext
add custom-dial-plan
   ID=cdp1;digit-string=*72;nod=VSC;fname=CFUA;cat-string=1111111111111111;
add custom-dial-plan
   ID=cdp1;digit-string=*73;nod=VSC;fname=CFUD;cat-string=1111111111111111;
add custom-dial-plan
   ID=cdp1;digit-string=*98;nod=VSC;fname=CFUI;cat-string=1111111111111111;
```

Call Hold

The Call Hold (CHD) feature allows a subscriber to temporarily shut off an active call, use the telephone to make another call, and then return to the original call, as well as alternate between the two.

**Note**
The CHD feature is for Centrex subscribers only. If a subscriber has both CW and CHD activated and they receive the CW tone, then the subscriber must hookflash and press *52 to switch to accept the new waiting call.

Prerequisites

None.

Supported Interfaces

Not applicable

Provisioning CHD

To provision CHD, perform the following steps:

**Step 1** Add the feature names.

```plaintext
add feature fname=CHD;tdpl=O_MID_CALL;tid1=O_SWITCH_HOOK_FLASH_IMMEDIATE;ttype1=R;
   tdp2=T_MID_CALL;tid2=T_SWITCH_HOOK_FLASH_IMMEDIATE;ttype2=R;feature-server-id=FSPTC235;des
   cription=Call Hold;grp-feature=N;
```

**Step 2** Create a service with the CHD feature.

```plaintext
add service id=548; fname1=CHD;
```
Step 3 Assign the service to the subscriber.

```
add subscriber-service-profile sub-id=ubr@cisco.com; service-id=548;
```

Call Park

The Call Park feature allows a subscriber (parking party) to park an active call against its own extension or another extension within the Call Park Subscriber Group (CPSG). Once a call is parked, the parking party is free to make other calls, while the parked party remains parked. The parked party can be retrieved by any subscriber within the CPSG; otherwise, the call is reoffered three times to the parking party.

Prerequisites

A subscriber or a group of subscribers with the Call Park feature. Subscribers must be provisioned as part of a CPSG. The subscribers must also be members of an existing Basic Business Group.

Supported Interfaces

Table 6-1 shows the interface support between call origination and termination.

<table>
<thead>
<tr>
<th></th>
<th>RGW termination</th>
<th>CAS termination</th>
<th>SS7 termination</th>
<th>ISDN termination</th>
<th>SIP termination</th>
</tr>
</thead>
<tbody>
<tr>
<td>RGW origination</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>CAS origination</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SS7 origination</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISDN origination</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP origination</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Provisioning Call Park

To provision the Call Park feature, perform the following steps:

Step 1 Add the announcement IDs for call park to the Call Agent Configuration table.

```
add ca-config type=cprk-ann; datatype=integer; value=901;
add ca-config type=cprk-clear; datatype=integer; value=902;
```
Call Transfer

The Call Transfer (CT) feature allows a subscriber to transfer an active call to a third party.

Prerequisites

None.

Supported Interfaces

Not applicable

Provisioning CT

To provision CT, perform the following steps:

**Step 1**  Add the feature.

```
add feature fname=CT; tdp1=O_MID_CALL; tid1=O_SWITCH_HOOK_FLASH_IMMEDIATE; ttype1=R;
tdp2=T_MID_CALL; tid2=T_SWITCH_HOOK_FLASH_IMMEDIATE; ttype2=R; feature-server-id=FSPTC235;
description=Call Transfer; grp-feature=N;
```
Step 2  Create a service with the Call Transfer feature.

   add service id=549; fname1=CT;

Step 3  Assign the service to the subscriber.

   add subscriber-service-profile sub-id=uhr@cisco.com; service-id=549;

---

**Call Waiting**

The Call Waiting (CW) service allows a subscriber to accept an incoming call, even when the subscriber is already involved in a call, and allows the subscriber to alternate between the two calls. When a subscriber is already involved in a call and a third person is trying to call them, then with the CW feature enabled the subscriber is notified with a tone of the new incoming call. The subscriber can then accept the call or ignore it. This way the subscriber does not miss any incoming calls.

A separate feature of Call Waiting is **Cancel Call Waiting** which is used when a subscriber does not wish to be notified of a waiting call. Cancel Call Waiting is on a per-call basis and must be activated prior to making a call.

**Prerequisites**

None.

**Supported Interfaces**

Not applicable

**Provisioning CW**

To provision CW, perform the following steps:

Step 1  Add the feature name.

   add feature fname=CW; tdp1=t-busy; tidi=t-busy; ttype1=R; description=Call Waiting;
   feature-server-id=FSPTC235;

Step 2  Add the service ID.

   add service id=1; fname1=CW

Step 3  Assign the service to the subscriber.

   add subscriber-service-profile sub-id=sub1; service-id=1;
Call Waiting Deluxe

The Call Waiting Deluxe (CWD) feature allows you to control how an incoming call(s) are handled when already on a two-way call.

Prerequisites

None.

Supported Interfaces

Not applicable

Provisioning CWD

To provision CWD, perform the following steps:

Step 1  Add the feature.

```plaintext
add feature fname=CWDA; tdp1=COLLECTED_INFORMATION; tid1=COLLECTED_INFORMATION; ttype1=R;
feature-server-id=FSPTC325;description=China Residential Call Waiting Deluxe Activation Feature;
add feature fname=CWDD; tdp1=COLLECTED_INFORMATION; tid1=COLLECTED_INFORMATION; ttype1=R;
feature-server-id=FSPTC325;description=China Residential Call Waiting Deluxe Deactivation Feature;
add feature fname=CWDI; tdp1=COLLECTED_INFORMATION; tid1=COLLECTED_INFORMATION; ttype1=R;
feature-server-id=FSPTC325;description=China Residential Call Waiting Deluxe Interrogation Feature;
add feature FNAME=CWD; tdp1=t-busy; tid1=t-busy; ttype1=R; feature-server-id=FSPTC325;
description=China Residential Call Waiting Deluxe Feature; fname1=CWDA; fname2=CWDD; fname3=CWDI
```

Step 2  Add the VSCs.

```plaintext
add vsc fname=CWDI;digit-string=*#58#;
add vsc fname=CWDA;digit-string=*58#;
add vsc fname=CWDD;digit-string=#58#;
```

Step 3  Create a service with the CWD feature.

```plaintext
add service id=1; FNAME1=CWD;
```

Step 4  Assign the service to the subscriber.

```plaintext
add subscriber-service-profile sub-id=china-1; service-id=1;
```
Provisioning CWD for Centrex Subscribers

To provision CWD for Centrex subscribers, perform the following steps:

**Step 1** Add the feature to the Custom Dial Plan table for the Centrex group.

```
add custom-dial-plan
id=cdp1;digit-string=*58#;nod=vsc;fname=CWDA;cat-string=1111111111111111;
add custom-dial-plan
id=cdp1;digit-string=#58#;nod=Vsc;fname=CWDD;cat-string=1111111111111111;
add custom-dial-plan
id=cdp1;digit-string=*#58#;nod=vsc;fname=CWDI;cat-string=1111111111111111;
```

Calling Identity Delivery and Suppression

The Calling Identity Delivery and Suppression (CIDS) feature allows a subscriber to explicitly specify on a per-call basis whether both calling name and calling number will be treated as private or public.

There are separate star codes for delivery or suppression. If you enter the code for delivery, then regardless of the subscriber’s default privacy, the name and number is treated as public. If you enter the code for suppression, then regardless of the default privacy, the subscriber’s name and number are treated as private.

**Prerequisites**

None.

**Supported Interfaces**

MGCP subscribers

**Provisioning CIDS**

To provision CIDS perform the following steps:

**Step 1** Add the feature name.

```
add feature fname=CIDSD; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R;
description=Calling Identity Delivery; feature-server-id=FSPTC235;
add feature fname=CIDSS; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R;
description=Calling Identity Suppression; feature-server-id=FSPTC235;
add feature fname=CIDS; fname1=CIDSD; fname2=CIDSS; feature-server-id=FSPTC235;
```
### Calling Identity Delivery on Call Waiting

The Calling Identity Delivery on Call Waiting (CIDCW) feature allows a subscriber to receive caller ID information about a calling party while talking to another party. This feature allows call waiting and caller ID to work together. If the subscriber is talking to one party and is alerted that another call is coming in, then the subscriber can see who is calling before deciding to put the current party on hold and taking the call.

**Prerequisites**

None.

**Supported Interfaces**

Not applicable

---

### Provisioning CIDS for Centrex Subscribers

To provision CIDS for a CENTREX group, perform the following steps:

---

**Step 1** Add the feature to the Custom Dial Plan table for the Centrex group.

```
add custom-dial-plan id=cdp1;digit-string=*82;nod=vsc;fname=CIDSD; cat-string=1111111111111111;
add custom-dial-plan id=cdp1;digit-string=*96;nod=vsc;fname=CIDSS; cat-string=1111111111111111;
```

---

### Calling Identity Delivery on Call Waiting

The Calling Identity Delivery on Call Waiting (CIDCW) feature allows a subscriber to receive caller ID information about a calling party while talking to another party. This feature allows call waiting and caller ID to work together. If the subscriber is talking to one party and is alerted that another call is coming in, then the subscriber can see who is calling before deciding to put the current party on hold and taking the call.

**Prerequisites**

None.

**Supported Interfaces**

Not applicable

---

### Provisioning CIDS for Centrex Subscribers

To provision CIDS for a CENTREX group, perform the following steps:

---

**Step 2** Add the VSCs.

```
add vsc digit-string=*82; fname=CIDSD;
add vsc digit-string=*96; fname=CIDSS;
```

**Step 3** Add the service ID.

```
add service id=2; fname1=CIDS;
```

**Step 4** Assign the service to the subscriber.

```
add subscriber-service-profile sub-id=rgw-19a@cisco.com; service-id=2;
```
Provisioning CIDCW

To provision CIDCW, perform the following steps:

**Step 1** Add the CIDCW feature name.

```
add feature fname=CIDCW; tdp1=t-busy; tid1=t-busy; ttype1=R; description=Caller Id with Call Waiting; feature-server-id=FSPTC235;
```

**Step 2** Add the service ID.

```
add service id=1; FNAME1=CIDCW; description=Common for All Subscribers;
```

**Step 3** Assign the service to the subscriber.

```
add subscriber-service-profile sub-id=135-14@ipclab.cisco.com; service-id=1;
```

Provisioning CIDCW for Centrex Subscribers

To provision CIDCW for Centrex subscribers, perform the following steps:

**Step 1** Assign the service to the subscriber.

```
add subscriber-service-profile sub-id=135-14@ipclab.cisco.com; service-id=1;
```

Calling Name Delivery

The Calling Name Delivery (CNAM) service delivers the name of the calling person, the telephone number, and the local date and time when the call was delivered, onto the telephone line. The telephone receiver must be equipped with a caller ID display device to view the information.

Prerequisites

The following steps are required before you can provision CNAM:

**Step 1** Add the global title and subsystem information into the Omni file, where the global title translation (GTT) = 8, and subsystem = 247.

```
LNP: CREATE-GT:TT=11,NP=ISDN-TEL,DIG="514606",PC=1-101-0,SSN=247,RI=DEF;
IN-800: CREATE-GT:TT=254,NP=ISDN-TEL,DIG="877",PC=1-101-0,SSN=254,RI=DEF;
CNAM: CREATE-GT:TT=5,NP=ISDN-TEL,DIG="408256",PC=1-101-0,SSN=232,RI=DEF;
```

Where:

- **CREATE-GT**—command
- **TT**—translation type
- **NP**—numbering plan
- **DIG**—digits
PC—destination point code
SSN—subsystem number
RI—Routing indicator.

Supported Interfaces
MGCP, ISDN, SS7

Provisioning CNAM
To provision CNAM, perform the following steps:

**Step 1** Add the CNAM feature names.
```
add feature fname=LIDB; tdp1=termination-attempt; tid1=CNAM; ttype1=R; description=LIDB
query for CNAM; feature-server-id=FSAIN205;
```
```
add feature fname=CNAM; tdp1=facility-selected-and-available; fname1=LIDB;
tid1=termination_resource_available; ttype1=R; description=Calling Name;
feature-server-id=FSPTC235;
```

**Step 2** Add the service ID.
```
add service id=10; fname1=CNAM; description=Common for All Subscribers;
```

**Step 3** Assign the service to the subscriber.
```
add sub-service-profile sub-id=xxx@ipclab.cisco.com; service-id=10;
```

Provisioning CNAM for Centrex Subscribers
To provision CNAM for Centrex subscribers, perform the following steps:

**Step 1** Assign the service to the subscriber.
```
add sub-service-profile sub-id=xxx@ipclab.cisco.com; service-id=10;
```
Calling Number Delivery

The Calling Number Delivery (CND) service brings the telephone number of the calling person, along with the local date and time when the call was delivered, onto called party’s telephone line. The telephone receiver must be equipped with a caller ID display device to view the information. The called party can then decide whether to accept the call, ignore the call, or ask some other person to pickup the call.

Prerequisites

Subscriber provisioning for POTS and Centrex members must be completed.

Supported Interfaces

Subscriber Line (MGCP) only.

Provisioning CND

To provision CND, perform the following steps:

**Step 1** Add the feature name.
```
add feature fname=CND; tdp1=facility-selected-and-available; tid1=termination-resource-available; ttype1=R; description=Calling number delivery; feature-server-id=FSPTC235
```

**Step 2** Add the service ID.
```
add service id=2; fname1=CND; description=CND for all SubscriberS;
```

**Step 3** Assign the service to the subscriber.
```
add sub-service-profile sub-id=rgw-3a@cisco.com; service-id=2;
```

Provisioning CND for Centrex Subscribers

To provision CND for Centrex subscribers, perform the following steps:

**Step 1** Assign the service to the subscriber.
```
add sub-service-profile sub-id=rgw-3a@cisco.com; service-id=2;
```
Calling Name Delivery Blocking

The Calling Name Delivery Blocking (CNAB) service allows a subscriber to toggle their calling name privacy status. That is, if calling number privacy is activated, using CNAB on the next call can make the calling name public. On the other hand, if calling name privacy is not activated, using CNAB can make the calling name of the next call private.

- If a subscriber’s telephone number is set to calling name public, the telephone number is delivered to the called party (the next dialed number), before going on-hook.
- If a subscriber’s telephone number is set to calling name private, the calling name is not displayed to the called party.

This service is activated on a per-call basis.

Prerequisites

None.

Supported Interfaces

Not applicable

Provisioning CNAB

To provision CNAB, perform the following steps:

---

**Step 1** Add the CNAB feature name.

```plaintext
add feature fname=CNAB; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R; feature-server-id=FSPTC235; description=CNAB;
```

**Step 2** Add the CNAB VSC.

```plaintext
add vsc fname=CNAB; digit-string=*95;
```

**Step 3** Add the service ID.

```plaintext
add service-id=1; fname1=CNAB;
```

**Step 4** Set the LIDB query flag for any Cisco BTS 10200 Softswitch POPs as required.

```plaintext
change pop id=1; cnam-option=LOCAL-OR-LIDB;
```

**Step 5** Assign the service to the subscriber.

```plaintext
add subscriber-service-profile sub-id=subscriber-1; service-id=1;
```
Provisioning CNAB for Centrex Subscribers

To provision CNAB for a Centrex subscriber, perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Add the feature into the Custom Dial Plan table for the Centrex group.</td>
<td><code>add custom-dial-plan ID=cdpl; digit-string=*95; nod=VSC; fname=CNAB; cat-string=111111111111111111111;</code></td>
</tr>
</tbody>
</table>

Calling Number Delivery Blocking

The Calling Number Delivery Blocking (CNDB) service allows a subscriber to toggle their telephone number privacy status. That is, if telephone number privacy is activated, using CNDB on the next call can make the telephone number public. On the other hand, if telephone number privacy is not activated, using CNAB can make the telephone number of the next call private.

- If a subscriber’s telephone number is set to telephone number public, the telephone number is delivered to the called party (the next dialed number), before going on-hook.
- If a subscriber’s telephone number is set to telephone number private, the telephone number is not displayed to the called party.

This service is activated on a per-call basis.

Prerequisites

None.

Supported Interfaces

Not applicable.

Provisioning CNDB

To provision CNDB, perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Add the CNDB feature name.</td>
<td><code>add feature fname=CNDB; Tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R; Feature-server-id=FSPTC235; description=CNDB;</code></td>
</tr>
<tr>
<td>2</td>
<td>Add the CNDB VSC.</td>
<td><code>add vsc fname=CNDB; digit-string=*67;</code></td>
</tr>
<tr>
<td>3</td>
<td>Add the service ID.</td>
<td><code>add service service-id=1; FNAME1=CNDB;</code></td>
</tr>
</tbody>
</table>
Assign the service to the subscriber.

```plaintext
add subscriber-service-profile sub-id=subscriber-1; service-id=1;
```

### Provisioning CNDB for Centrex Subscribers

To provision CNDB for a Centrex subscriber, perform the following steps:

#### Step 1
Add the feature into the Custom Dial Plan table for the Centrex group.

```plaintext
add custom-dial-plan ID=cdp1; digit-string=*67; nod=vsc; FNAME=CNDB;
cat-string=1111111111111111;
```

### Cancel Call Waiting

The Cancel Call Waiting (CCW) service allows a subscriber to turn off the existing Call Waiting service for either the duration of a current call or for the next call.

#### Prerequisites
None.

#### Supported Interfaces
Not applicable

### Provisioning CCW

To provision CCW, perform the following steps:

#### Step 1
Add the CCW feature names. If call waiting has already been provisioned, omit the first command.

```plaintext
add feature fname=CW; tdp1=t-busy; tid1=t-busy; ttype1=R; description=Call Waiting;
feature-server-id=FSPTC235;
add feature fname=CCW; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R;
description=Cancel Call Waiting; feature-server-id=FSPTC235;
```

#### Step 2
Add the VSC.

```plaintext
add vsc digit-string=*70;fname=CCW
```

#### Step 3
Add the service ID.

```plaintext
add service id=1; fname1=CCW; fname2=CW
```

#### Step 4
Assign the service to the subscriber.
add subscriber-service-profile sub-id=test; service-id=1; priority=1;

Provisioning CCW for Centrex Subscribers

To provision CCW for Centrex subscribers, perform the following steps:

**Step 1** Add feature into the custom-dial-plan table for the centrex group.
add cdp; id=cdp1; digit-string=9; nod=POTS-ACCESS; cat-string=1111111111111111;

Centrex Direct Inward Dial and Direct Outward Dial

The Direct Inward Dial (DID) service provides a Centrex group with the ability to receive a call from the PSTN without attendant intervention. The Direct Outward Dial (DOD) services provides a Centrex group with the ability to make a call to the PSTN without attendant intervention.

Prerequisites

None.

Supported Interfaces

MGCP subscribers.

Provisioning Centrex DID and DOD

To provision Centrex DID and DOD, perform the following steps:

**Step 1** Add feature into the custom-dial-plan table for the centrex group.
add cdp; id=cdp1; digit-string=9; nod=POTS-ACCESS; cat-string=1111111111111111;

Centrex Extension Dial

The Centrex Extension Dial (CED) service allows subscribers within a Centrex group to call each other by dialing only a portion of the telephone number. It also allows you to set the number of incoming and outgoing simultaneous calls from a Centrex group using the incoming simulated facility group (ISFG) and outgoing simulated facility group (OSFG) features.
Prerequisites

None.

Supported Interfaces

MGCP subscribers

Provisioning CED

To provision CED, perform the following steps:

**Step 1**
Add the feature names incoming simulated facility group outgoing.

```plaintext
add feature fname=ISFG; tdp1=TERMINATION_ATTEMPT_AUTHORIZED; tid1=TERMINATION_ATTEMPT_AUTHORIZED; ttype1=R; description=Incoming SFG; feature-server-id=FSPTC235;

add feature fname=OSFG; tdp1=route-selected; tid1=route-selected; ttype1=R; description=Outgoing SFG; feature-server-id=FSPTC235;

add feature; fname=CDP; TDP1=COLLECTED_INFORMATION; TID1=CUSTOMIZE_DIALING_PLAN; ttype1=R; feature-server-id=FSPTC325; description=Customize Dial Plan;

add service id=3; fname1=ISFG; fname2=OSFG; fname3=CDP;
```

**Note**
If the PAC is 9, then |9| must be in the digit map.
If the PAC is 8, then |8| must be in the digit map.
If an extension dial needs 4D, then |4xxx| must be in the digit map.

**Step 2**
Add the custom dial plan profile ID.

```plaintext
add custom-dial-plan-profile id=cdp1;
```

**Step 3**
Add the Centrex group ID.

```plaintext
add ctxg idCTXgroup; da-cwi=N; SFG-CONTROL=Y; cat-screening=Y; internal-cnd-only=N; in-sfg-count=2; out-sfg-count=2; both-sfg-count=4; cdp-id=cdp1; main-sub-id=sub1-ctx; call-agent-id=CA166;
```

**Step 4**
Add the CDP ID.

a. For 3-digit extension dialing. If 4-digit dialing is required, go to Step b.

```plaintext
add cdp id=cdp1; digit-string=4xx; nod=EXTENSION; cat-string=111111111111111111;
```

b. For 4-digit extension dialing.

```plaintext
add cdp id=cdp1; digit-string=4xxx; nod=EXTENSION; cat-string=111111111111111111;
```

c. If PAC = 9.

```plaintext
add cdp id=cdp1; digit-string=9; nod=POTS-ACCESS; cat-string=111111111111111111;
```

d. If PAC = 8.
add cdp id=cdp1; digit-string=8; nod=POTS-ACCESS; cat-string=11111111111111;
Step 5  Assign the Centrex subscribers to the Centrex Group.

```
change sub id=sub1-ctx; ctxg-id=CTXgroup;
change sub id=sub2-ctx; ctxg-id=CTXgroup;
```

Step 6  Assign extensions to the subscriber.

```
add ext2subscriber ctxg-id=CTXgroup; ext=0;
assigned=Y;ctx-restrict=NONE;attendant=N;cat-code=1;sub-id=sub1-ctx;

add ext2subscriber ctxg-id=CTXgroup; Ext=412;assigned=Y;ctx-restrict=NONE;attendant=N;
cat-code=1;sub-id=sub2-ctx;
```

---

## Centrex POTS Access Code

The Centrex POTS Access Code (PAC) feature allows a subscriber to use an access code to dial a designated area within the Centrex group.

### Prerequisites

None.

### Supported Interfaces

MGCP subscribers

### Provisioning Centrex PAC

To provision a Centrex PAC, perform the following steps:

---

**Step 1**  Add POTS access into the custom-dial-plan table for the Centrex group.

```
add cdp; id=cdp1; digit-string=9; nod=POTS-ACCESS; cat-string=1111111111111111;
```

---

## Class of Service

The Class of Service (COS) service provides call screening based on the class of service assigned to a telephone number.

### Prerequisites

None.
Supported Interfaces

SS7, MGCP, ISDN, CAS

Provisioning Office COS

To provision office COS, perform the following steps:

**Step 1** Register the feature in the Office.

```plaintext
add feature FNAME=COS;tdp1=COLLECTED_INFORMATION; tid1=COS-TRIGGER; ttype1=R;
feature-server-id=FSPTC235; description=Class Of Service; grp-feature=N;
```

**Step 2** Provision the feature into a service package.

```plaintext
add service id=special-srv; fname1=COS;
```

**Step 3** Provision a class of service restriction class.

```plaintext
add cos-restrict id=new-age-restrict;
casual-restrict-type=<applicable-values>;nanp-restrict-type=<applicable-values>;
nanp-wb-list=<applicable-values>;intl-restrict-type=<applicable-values>;
i2-restrict=<applicable-values>;nod-wb-list=<applicable-values>;
acct-code-allow=<applicable-values>;acct-code-length=<applicable-values>;
auth-code-allow=<applicable-values>;auth-code-length=<applicable-values>;
auth-code-grp-id=<applicable-values>
```

**Step 4** Provision COS Restrict related tables based on the following cos-restrict tables.

- Auth-code-grp
- Auth-code
- Casual-wb-list
- Intl-wb-list
- Lata
- Lata-map
- Nanp-wb-list

**Note** Refer to the *Cisco BTS 10200 Softswitch Command Line Reference Guide* for specific cos-restrict table information.

**Step 5** Provision COS on a given trunk group if required.

```plaintext
add trunk-grp-feature-data tgn-id=isdn-1;tg=isdn-trunk-1;casual-call=Y/N;
cos-restrict-id=new-age-restrict;
```
Provisioning COS for Subscriber, Centrex and MLHG

To provision COS for subscriber, Centrex, and MLHG, perform the following steps:

**Step 1** Add the trunk group feature data ID.
```
add trunk-grp-feature-data tgn-id=3; cos-restrict-id=SS7-LOCAL1;
```

**Step 2** Add the trunk group service profile ID.
```
add trunk-grp-service-profile tgn-id=3; service-id=21; priority=1;
```

*Note* The trunk group service profile is for an incoming SS7 on tgn-id=3.

**Step 3** Add the service to the subscriber's service profile.
```
add subscriber-service-profile sub-id=sub1-plano.com; service-id=special-srv;
```

**Step 4** Add the COS restrict ID to the Subscriber table.
```
add subscriber sub-id=sub1-plano.com; cos-restrict-id=new-age-restriction;
```

Codec Negotiation

The Codec Negotiation (CN) feature is a process used during call transition states to change from a previously selected codec to a different one. CN allows calls to be started using a certain low-speed codec (for example, on-net calls). Then, depending on the features used, if a different codec is needed to complete the feature call, CN switches the call to another codec. Thus, a codec is first selected and then negotiated as necessary for transition states in the call.

Prerequisites

In the Media Gateway Profile table, codec-neg-unsupp must be N (no).

In the Call Agent Configuration table, codec-mod-during-call must Y (yes).

Supported Interfaces

Not applicable
Provisioning Codec Negotiation

To provision Codec Negotiation, perform the following steps:

**Step 1**
Add the quality of service ID.
```
add qos id=CODEC-PCMU;codec-type=G711U;rsvp-required=N;resource-reservation=BE;
```

**Step 2**
Associate the Quality of Service id to the subscriber
```
change sub id=x;qos-id=CODEC-PCMU
```

Codec Selection

The Codec Selection (CS) feature allows specifying a preferred codec for call establishment using a variety of encoding and decoding algorithms to compress voice for transmission using the realtime transport protocol (RTP).

Prerequisites

None.

Supported Interfaces

Not applicable

Provisioning CS

To provision CS, perform the following step:

**Step 1**
Add the quality of service ID.
```
add qos ID=CODEC-PCMU;codec-type=G711U;rsvp-required=N;resource-reservation=BE;
```

**Step 2**
Associate the QoS id to the subscriber.
```
change subscriber id=sub1;qos-id=CODEC-PCMU;
```

**Step 3**
Associate the Qos id to the trunk (optional).
```
change tgn-id=124; qos-id=CODEC-PCMU;
```
Customer Originated Trace

The Customer Originated Trace (COT) feature allows subscribers to generate a record of an incoming harassing call. The date and time of the trace, the calling DN, the unique/nonunique nature of the calling DN, the customer's DN, the customer's termination ID, answer indication, call-waited indication, and the date/time of the call are all recorded. This feature works with announcements or tones to prompt the subscriber to generate a trace.

Prerequisites

A subscriber must be assigned with the Customer Origination Trace feature.
A set of announcements must be provisioned for COT (70, 71, 72, 73, 74, and 75). Refer to Chapter 7, “Provisioning Announcements” for more details.

Supported Interfaces

Table 6-2 shows the interface support between call origination and termination.

<table>
<thead>
<tr>
<th>Table 6-2 Customer Originated Trace Supported Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>RGW termination</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>RGW origination</td>
</tr>
<tr>
<td>CAS origination</td>
</tr>
<tr>
<td>SS7 origination</td>
</tr>
<tr>
<td>ISDN origination</td>
</tr>
<tr>
<td>SIP origination</td>
</tr>
</tbody>
</table>

Provisioning a COT

To provision a COT, perform the following steps:

1. Add the announcement for `cot_ann_trace_dn_is_ou` (cause code 1061) and its associated release cause code ID.

```
add announcement id=75; type=system; send-answer=n; num-repeat=1; duration=20;
announcement-file=ann_id_75.au; route-guide-id=annc5-rg; announcement-number=75;
add release-cause id=1061; annn-id=75;
```
**Step 2**  Add the announcement for cot_ann_trace_success (cause code 1062) and its associated release cause code ID.

```
add announcement id=70; type=system; send-answer=n; num-repeat=1; duration=20;
announcement-file=ann_id_70.au; route-guide-id=annc5-rg; announcement-number=70;
add release-cause id=1062; annn_id=70;
```

**Step 3**  Add the announcement for cot_ann_trace_denied (cause code 1063) and its associated release cause code ID.

```
add announcement id=71; type=system; send-answer=n; num-repeat=1; duration=20;
announcement-file=ann_id_71.au; route-guide-id=annc5-rg; announcement-number=71;
add release-cause id=1063; annnc_id=71;
```

**Step 4**  Add the announcement for cot_ann_trace_try_again (cause code 1064) and its associated release cause code ID.

```
add announcement id=72; type=system; send-answer=n; num-repeat=1; duration=20;
announcement-file=ann_id_72.au; route-guide-id=annc5-rg; announcement-number=72;
add release-cause id=1064; annnc_id=72;
```

**Step 5**  Add the announcement for cot_ann_trace_buffer_empty (cause code 1065) and its associated release cause code ID.

```
add announcement id=73; type=system; send-answer=n; num-repeat=1; duration=20;
announcement-file=ann_id_73.au; route-guide-id=annc5-rg; announcement-number=73;
add release-cause id=1065; annnc_id=73;
```

**Step 6**  Add the announcement for cot_ann_trace_dn_already_done (cause code 1066) and its associated release cause code ID.

```
add announcement id=74; type=system; send-answer=n; num-repeat=1; duration=20;
announcement-file=ann_id_74.au; route-guide-id=annc5-rg; announcement-number=74;
add release-cause id=1066; annnc_id=74;
```

**Step 7**  Set the COT level activation to **one** or **two**.

```
add ca-config cot-activation-level; datatype=string; value=TWO;
```

**Step 8**  Add the feature name.

```
add feature;fname=COT; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R;
feature-server-id=FSPTC235;
```

**Step 9**  Add the VCS digit string for the COT access code.

```
add vsc digit-string=*57; fname=COT;
```

**Step 10**  Add the customer originated trace service ID and assign it to a subscriber.

```
add service id=45; fname1=COT;
add subscriber-service-profile sub-id=subl-pots; service-id=45;
```
Provisioning Centrex COT

To provision a Centrex COT, perform the following steps:

**Step 1**
Add COT into the custom-dial-plan table for the Centrex group.

```
add cdp; id=cdp1; fname=COT; digit-string=*57; nod=VSC; cat-string=1111111111111111;
```

Direct Inward Dial Foreign Exchange Office

The Direct Inward Dial (DID) Foreign Exchange Office (FXO) feature allows a subscriber to place a local call and have that call go through a central office outside of his local exchange area.

Prerequisites

None.

Supported Interfaces

MGCP FXO port only

Provisioning DID FXO

To provision DID FXO, perform the following steps:

**Step 1**
Add the MGW profile.

```
add mgw-profile id=fxo-mgp1; vendor=cisco; silent-suppress-supp=y; fxo=y; fxs=n; description=FXO testing;
```

**Step 2**
Add the MGW.

```
add mgw id=2420-187; tsap-addr=10.89.227.187; call-agent-id=CA166; mgw-profile-id=fxo-mgp1; status=OOS; call-agent-control-port=0; mgw-backhaul-port=22; call-agent-backhaul-port=33; rgw=y; tgw=n; nas=n; iad=n; pbx=y; ans=n; ivr=n;
```

**Step 3**
Add the CAS TG profile ID(s).

```
add cas-tg-profile id=fxo-dtmf-im; type=dtmf-imstart; oss-sig=y; test-line=n;
add cas-tg-profile id=fxo-dtmf-wink; type=dtmf-winkstart; oss-sig=y; test-line=n;
add cas-tg-profile id=fxo-mf-im; type=mf-imstart; oss-sig=y; test-line=n;
add cas-tg-profile id=fxo-mf-wink; type=mf-winkstart; oss-sig=y; test-line=n;
```

**Step 4**
Add the trunk group ID.

```
add trunk-grp id=151; call-agent-id=CA166; tg-type=CAS; dial-plan-id=dp1; status=OOS; sel-policy=LRU; direction=out; glare=ODD; tg-profile-id=fxo-dtmf-im;
```
Step 5  Add the termination prefix.
add termination prefix=aaln/S1/;port-start=5;port-end=5;mgw-id=2420-187;
type=trunk;mgcp-pkg-type=dt;status=ooos;

Step 6  Add the office code digit string.
add office-code digit-string=972-614;office-code-index=23;did=Y;

Step 7  Add the route ID(s).
add route id=fxo-rt;1cr=Y;tgn1-id=151;
add route-guide id=fxo-rd;policy-type=ROUTE;policy-id=fxo-rt;

Step 8  Add the subscriber and assign the FXO main-sub-id to the trunk group.
add subscriber id=fxo-sub1;category=pbx;name=fxo-sub1;status=active;privacy=none;
ring-type-dn1=1;ring-type-dn2=2;ring-type-dn3=3;billing-dn=972-614-0000;term-id=aaln/S1/5;
mgw-id=2420-187;tgn-id=151;usage-sens=n;sub-profile-id=dp1;term-type=route;
policy-id=fxo-rt;
change trunk-grp id=151;call-agent-id=CA166;main-sub-id=fxo-sub1;

Step 9  Add the trunk termination prefix and assign the trunk to the termination.
add trunk termination-prefix=aaln/S1/;termination-port-start=5;
termination-port-end=5;cic-start=5;cic-end=5;tgn-id=151;mgw-id=2420-187;
change termination id=aaln/S1/5;mgw-id=2420-187;trunk-id=5;tgn-id=151;

Step 10 Add the DN2Subscriber office code index.
add dn2subscriber office-code-index=23;dn=XXXX;sub-id=fxo-sub1;

Step 11 Add the destination ID.
add destination dest-id=fxo-dest;call-type=local;route-type=sub;
office-code-index=23;zero-plus=n;intra-state=n;description=dummy;

Step 12 Add the dial plan ID.
add dial-plan id=dp1;digit-string=972-614;reqd-digits=10;dest-id=fxo-dest;

Directed Call Pickup With and Without Barge-in

The Directed Call Pick-Up (DPN) feature allows a subscriber in a basic business group (BBG) to answer a call to a telephone from another telephone within the business group. DPN has two versions: without barge-in capability (DPN) and with barge-in capability (DPU).

Note  This feature is applicable only to Centrex subscribers.

Prerequisites

The Centrex group must be provisioned.
Supported Interfaces

Centrex Subscriber Line (MGCP) only

Provisioning DPN and DPU

This section describes how to provision DPN and DPU.

Provisioning DPN

To provision DPN, perform the following steps. This feature is assigned to a subscriber to invoke call pickup.

Step 1  Add the feature name.
        \texttt{add feature fname=DPN; feature-server-id=FSPTC235; description=Directed Call Pickup Without Barge-in;}

Step 2  Add the service ID.
        \texttt{add service id=42; fname1=DPN}

Step 3  Add the CDP ID.
        \texttt{add cdp id=135-ctx; digit-string=*23; nod=vsc; fname=DPN; cat-string=111111111111111111111}

Step 4  Add the subscriber service profile subscriber ID.
        \texttt{add sub-service-profile sub-id=rgw-2421-1@cisco.com; service-id=42;}

Provisioning DPU

To provision DPU, perform the following steps. This feature is assigned to a subscriber who will be picked up.

Step 1  Add the feature name.
        \texttt{add feature fname=DPU; feature-server-id=FSPTC235; description=Directed Call Pickup With Barge-in;}

Step 2  Add the service ID.
        \texttt{add service id=43; fname1=DPU}

Step 3  Add the CDP ID.
        \texttt{add cdp id=135-ctx; digit-string=*24; nod=vsc; fname=DPU; cat-string=111111111111111111111}

Step 4  Assign the service to the subscriber.
        \texttt{add sub-service-profile sub-id=rgw-2421-2@cisco.com; service-id=43;}
Distinctive Alerting Call Waiting Indicator

The Distinctive Alerting Call Waiting Indicator (DACWI) feature provides Centrex subscribers with special ringing and call waiting tones on DID calls.

**Note**
This feature is applicable only to Centrex subscribers.

**Prerequisites**

Call Waiting feature must be provisioned.
A Centrex group must be provisioned.

**Supported Interfaces**

MGCP

**Provisioning a DACWI**

To provision DACWI, perform the following steps:

**Step 1** Add the feature name.
```
add feature fname=DACWI;tdp1=TERMINATION_ATTEMPT_AUTHORIZED;
tid1=TERMINATION_ATTEMPT_AUTHORIZED; ttype1=R; description=Distinctive Alerting Call Waiting Indication; feature-server-id=FSPTC235;
```

**Step 2** Add the service ID.
```
add service id=1; fname1=CW;fname2=DACWI;
```

**Step 3** Assign the service to the subscriber.
```
add subscriber-service-profile sub-id=ctx-sub2b@cisco.com; service-id=1;
```

Distinctive Ringing Call Waiting

The Distinctive Ringing Call Waiting (DRCW) service allows a subscriber to define a list of telephone numbers. Incoming calls that are on the list have a distinctive ring for an incoming call when the line is idle, or a distinctive call waiting tone when the subscriber is in a call. Incoming calls not on the list are unaffected.

**Prerequisites**

A media server database (IVR) must be set up.
Supported Interfaces

MGCP

Provisioning DRCW

To provision DRCW, perform the following steps:

**Step 1**
Add the feature name.

```plaintext
add feature fname=DRCW_ACT; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R; tdp2=T_ANSWER; tid2=T_ANSWER; ttype2=R; description=DRCW Activation; feature-server-id=FSPTC235;
add feature fname=DRCW; TDP1=TERMINATION_ATTEMPT_AUTHORIZED; TID1=TERMINATION_ATTEMPT_AUTHORIZED; ttype1=R; FEATURE_SERVER_ID=FSPTC235; DESCRIPTION=Distinctive Ringing/Call Waiting;
```

**Step 2**
Add the service ID.

```plaintext
add service id=52; fname1=DRCW; fname2=DRCW_ACT; description=Common for all subscribers;
```

**Step 3**
Add the VSC digit strings.

```plaintext
add vsc digit-string=*61; fname=DRCW_ACT;
add vsc digit-string=*81; fname=DRCW_ACT;
```

**Step 4**
Assign the service to the subscriber.

```plaintext
add subscriber-service-profile sub-id=ctx-sub2b@cisco.com; service-id=52;
```

Provisioning Centrex DRCW

To provision a Centrex DRCW, perform the following steps:

**Step 1**
Add DRCW into the custom-dial-plan table for the Centrex group.

```plaintext
add cdp; id=cdp1; digit-string=*61; fname=DRCW_ACT; nod=VSC; cat-string=11111111111111111;
add cdp; id=cdp1; digit-string=*81; fname=DRCW_ACT; nod=VSC; cat-string=11111111111111111;
```

Do Not Disturb

The Do Not Disturb (DND) feature routes incoming calls either to a special Do Not Disturb Announcement or to a special tone.

Prerequisites

None.
Chapter 6  Provisioning Features and Services

Do Not Disturb

Supported Interfaces

Not applicable

Provisioning DND

To provision DND, perform the following steps:

---

**Step 1**
Add the feature name.

```
add feature fname=DND_ACT; TDP1=COLLECTED_INFORMATION; TID1=VERTICAL_SERVICE_CODE; ttype1=R; FEATURE_SERVER_ID=FSPTC235; DESCRIPTION=DND Activation;
```

```
add feature fname=DND_DEACT; TDP1=COLLECTED_INFORMATION; TID1=VERTICAL_SERVICE_CODE; ttype1=R; FEATURE_SERVER_ID=FSPTC235; DESCRIPTION=DND Deactivation;
```

```
add feature fname=DND; tdp1=TERMINATION_ATTEMPT_AUTHORIZED; ttd1=TERMINATION_ATTEMPT_AUTHORIZED; ttype1=R; fname1=DND_ACT; fname2=DND_DEACT; feature-server-id=FSPTC235; description=Do not disturb; grp-feature=N;
```

---

**Step 2**
Add the VSC digit strings.

```
add VSC digit-string=*78; fname=DND_ACT
add VSC digit-string=*79; fname=DND_DEACT
add VSC digit-string=1178; fname=DND_ACT
add VSC digit-string=1179; fname=DND_DEACT
```

---

**Step 3**
Add the service ID.

```
add service id=7; fname=DND;
```

---

**Step 4**
Assign the service to the subscriber.

```
add sub-service-profile sub-id=X; service-id=7;
```

---

Provisioning Centrex DND

To provision a Centrex DND, perform the following steps:

---

**Step 1**
Add DND into the custom-dial-plan table for the Centrex group.

```
add cdp; id=cdp1; digit-string=*78; fname=DND_ACT; nod=VSC; cat-string=1111111111111111;
add cdp; id=cdp1; digit-string=*79; fname=DND_DEACT; nod=VSC; cat-string=1111111111111111;
```
Dual Tone Multifrequency Relay

The Dual Tone Multifrequency (DTMF) Relay feature specifies what dual tone multifrequency (DTMF) to use between endpoints for a call. Use the `mgcp dtmf-relay` command in the gateway to enable this feature. To disable this feature for noncompressed codecs, use the `no` form of this command in the gateway. Provisioning DTMF is done from the gateway.

Prerequisites

None.

Supported Interfaces

Not applicable

Provisioning DTMF Relay

To provision DTMF Relay in the Cisco BTS 10200 Softswitch, perform the following step:

Step 1 Add the DTMF Relay feature to the MGW Profile. This command example is for an MGCP-to-MGCP scenario.

```
change mgw-profile id=XXX; dtmf-gwmode-supp=Y; dtmf-camode-supp=N;
dtmf-oob=y;dtmf-pref-mode=dtmf-oob;
```

Hotline

The Hotline feature allows a subscriber to connect to a predefined telephone number by just lifting the handset. The hotline feature can be used as a special high-priority line or for a frequently called number.

Prerequisites

An exclusive telephone connection is required.

Supported Interfaces

Hotline originations are supported only on subscriber line interfaces.
Provisioning Hotline

To provision Hotline, perform the following steps:

**Step 1** Add the feature.
```
add feature fname=HOTLINE; tdp1=o-attempt-authorized; tid1=o-attempt-authd; ttype1=R;
feature-server-id=FSPTC235; description=Hotline; grp-feature=N;
```

**Step 2** Provision the feature into a service package.
```
add service id=555; fname=HOTLINE;
```

**Step 3** Add the service to the subscriber's service profile.
```
add subscriber-service-profile sub-id=24h1-14@ipclab.cisco.com; service-id=555
```

**Step 4** Add the Hotline target DN to the subscriber's feature data.
```
add subscriber-feature-data sub-id=24h1-14@ipclab.cisco.com; fname=HOTLINE; type1=fdn1;
value1=9722132401;
```

Provisioning Hotline for Centrex

To provision Hotline for Centrex, perform the following steps:

**Step 1** Add the Hotline target DN to the subscriber's feature data.
```
add subscriber-feature-data sub-id=24h1-14@ipclab.cisco.com; fname=HOTLINE; type1=fdn1;
value1=9722132401;
```

**Step 2** Add the service to the subscriber's service profile.
```
add subscriber-service-profile sub-id=24h1-14@ipclab.cisco.com; service-id=555
```
Local Number Portability

The Local Number Portability (LNP) service allows subscribers to keep their phone numbers after changing service providers or location. An LNP query is sent to the Service Control Point (SCP) if the called (dialed) number is ported. The SCP response to the query is used to route the call.

Prerequisites

The following step is required before you can provision LNP:

Step 1: Add the global title and sub system information into the Omni file, where the global title translation (GTT) = 8, and subsystem = 247.

```
LNP: CREATE-GT:TT=11,NP=ISDN-TEL,DIG="514606",PC=1-101-0,SSN=247,RI=DEF;
IN-800: CREATE-GT:TT=254,NP=ISDN-TEL,DIG="877",PC=1-101-0,SSN=254,RI=DEF;
CNAM: CREATE-GT:TT=5,NP=ISDN-TEL,DIG="408256",PC=1-101-0,SSN=232,RI=DEF;
```

Where:
- CREATE-GT—command
- TT—translation type
- NP—numbering plan
- DIG—digits
- PC—destination point code
- SSN—subsystem number
- RI—Routing indicator.

Supported Interfaces

MGCP, ISDN, SS7

Provisioning LNP

To provision LNP, perform the following steps:

Step 1: Add the feature name.

```
add feature fname=LNP; tdp1=COLLECTED_INFORMATION; tid1=LNP-TRIGGER; ttype1=R;
description=Local Number Portability; feature-server-id=FSAIN205;
```
## Multiline Hunt Group

A Multiline Hunt Group (MLHG) is a telecommunications channel between two points, such as a telephone company central office (CO) or switching center, and a call center, PBX, or key system. Typically, a business has more stations (telephones) than lines, and hunting features allow sharing of a group of lines by many individual stations for both incoming and outgoing calls. A hunt group is simply a series of lines organized in such a way that if the first line is busy, the next line is hunted, and so on, until a free line is found. This arrangement is often used on a group of incoming lines.

### Prerequisites

None.

### Supported Interfaces

MGCP

### Provisioning a POTS MLHG

To provision the POTS MLHG feature, perform the following steps:

**Step 1** Add the subscriber ID.

```plaintext
add sub id=mlhgterm1; category=mlhg; status=active; name=mlhgterm1;
billing-dn=972-255-1230; dn1=972-255-1231; privacy=none; term-id=aaln/s1/1;
mgw-id=c2421.135; pic1=3333; pic2=2222; pic3=9999; grp=n; usage-sens=y;
sub-profile-id=sp7;
```

```plaintext
add sub id=mlhgterm2; category=mlhg-individual; status=active; name=mlhgterm2;
billing-dn=972-255-1230; dn1=972-255-1232; privacy=none; term-id=aaln/s1/2;
mgw-id=c2421.135; pic1=3333; pic2=2222; pic3=9999; grp=N; usage-sens=Y;
sub-profile-id=sp7;
```

**Step 2** Add the MLHG ID.

```plaintext
add mlhg id=mlhg1; hunt-type=regular; max-lines=10; call-agent-id=CA166;
main-sub-id=mlhgterm1;
```

**Step 3** Assign the subscriber ID to the MLHG.

```plaintext
change sub id=mlhgterm1; mlhg-id=mlhg1;
change sub id=mlhgterm2; mlhg-id=mlhg1;
```
**Chapter 6 Provisioning Features and Services**

### Multiline Hunt Group

**Step 4** Add the MLHG terminal MLHG ID.

```plaintext
add mlhg-terminal mlhg-id=mlhg1;terminal=1;term-id=aaln/S1/1;mgw-id=c2421.135
add mlhg-terminal mlhg-id=mlhg1;terminal=2;term-id=aaln/S1/2;mgw-id=c2421.135
```

---

### Provisioning a Centrex MLHG

To provision a Centrex group MLHG, perform the following steps:

**Step 1** Add the custom dial plan profile ID.

```plaintext
add custom-dial-plan-profile id=ctxg-mlhg-cdp1;
```

**Step 2** Add the CDP ID.

```plaintext
add cdp id=ctxg-mlhg-cdp1; digit-string=7xx;nod=EXTENSION;cat-string=1111111111;
add cdp id=ctxg-mlhg-cdp1; digit-string=9;nod=POTS-ACCESS;cat-string=1111111111111111;
add cdp id=ctxg-mlhg-cdp1; digit-string=0;nod=ATTENDANT-ACCESS;
cat-string=1111111111111111;
```

**Step 3** Add the first subscriber ID.

```plaintext
add subscriber id=ctx-mlhg-5; category=ctxg-mlhg; name=ctx-mlhg-5; status=ACTIVE;
address1=1651 n glenville suite 200; address2=Richardson tx 75081; ss-number=000-99-9999;
sip-url=/gateway21.home.com; billing-dn=214-255-2705; dn1=214-255-2705; ring-type-dn1=1;
term-id=aaln/S1/5; sub-profile-id=sp8; mgw-id=c2421.135; grp=n;
```

**Step 4** Add the Centrex group ID.

```plaintext
add ctxg id=ctxg-mlhg1; sfg-control=Y; in-sfg-count=4; out-sfg-count=4; both-sfg-count=4;
cdp-id=ctxg-mlhg-cdp1; call-agent-id=CA166; main-sub-id=ctx-mlhg-5;
```

**Step 5** Add the second subscriber ID.

```plaintext
add subscriber id=ctx-mlhg-6; category=ctxg-mlhg; name=ctx-mlhg-6; status=ACTIVE;
address1=1651 n glenville suite 200; address2=Richardson tx 75081; ss-number=000-99-9999;
sip-url=/gateway22.home.com; billing-dn=214-255-2706; dn1=214-255-2706; ring-type-dn1=1;
term-id=aaln/S1/6; sub-profile-id=sp8; mgw-id=c2421.135;
```

**Step 6** Assign the Centrex group ID to the subscribers.

```plaintext
change sub id=ctx-mlhg-5; ctxg-id=ctxg-mlhg1;
change sub id=ctx-mlhg-6; ctxg-id=ctxg-mlhg1;
```

**Step 7** Add the MLHG.

```plaintext
add mlhg id=ctxg-mlhg1; hunt-type=regular; max-lines=10; call-agent-id=CA166;
main-sub-id=ctxg-mlhg-5;
```

**Step 8** Assign the MLHG ID to the subscribers.

```plaintext
change sub id=ctx-mlhg-5; mlhg-id=ctxg-mlhg1;
change sub id=ctx-mlhg-6; mlhg-id=ctxg-mlhg1;
```

**Step 9** Add the MLHG terminal MLGH ID.

```plaintext
add mlhg-terminal mlhg-id=ctxg-mlhg1; terminal=1; term-id=aaln/S1/5; mgw-id=c2421.135
add mlhg-terminal mlhg-id=ctxg-mlhg1; terminal=2; term-id=aaln/S1/6; mgw-id=c2421.135
```
Multiple Directory Number

The Multiple Directory Number (MDN) feature allows three directory numbers (DNs) to be assigned to a single telephone line. Each individual DN is recognized using a special alerting pattern. One of the three DNs is designated as a primary DN during subscription.

Prerequisites

None.

Supported Interfaces

Subscriber Line (MGCP)

Provisioning an MDN

To provision an MDN, perform the following steps:

Step 1  Add the feature name.

```
add feature fname=MDN;tdp1=TERMINATION_ATTEMPTAUTHORIZED;
tid1=TERMINATION_ATTEMPTAUTHORIZED; ttype1=R; description=MultipleDirectoryNumbers;
feature-server-id=FSPTC235;
```

Step 2  Add the service ID.

```
add service id=56; fname=MDN;
```

Step 3  Assign the service to the subscriber.

```
add sub-service-profile sub-id=c421-121-5@cisco.com; service-id=56;
```

Step 4  Add the subscriber feature data subscriber ID.

```
add subscriber-feature-data sub-id=c421-121-5@cisco.com; fname=MDN; type1=fdn1;
value1=2142711005; type2=fdn2; value2=24271105; type3=fdn3; value3=2142711025;
```
Network Access Server

The MGCP Network Access Server (NAS) feature allows the Call Agent to pass additional incoming call information such as calling- and called-party-to-number to the media gateway for preauthentication (authorization) of modem and data calls.

Prerequisites

The NAS token in the Media Gateway table must be set to Y (yes).

Supported Interfaces

MGCP, SS7

Provisioning NAS

To provision NAS, perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Add a MGW.</td>
</tr>
</tbody>
</table>
| | ```
add mgw id=c2421.192;tsap-addr=c2421.192.trnglab.cisco.com;call-agent-id=CA101;
mgw-profile-id=IAD2421; type=rgw;nas=y;
``` |
| **Step 2** | Add the MGW profile ID. |
| | ```
add mgw-profile id=IAD2421; vendor=Cisco; packet-type=IP;mgcp-variant=NONE;aal1=n; aal2=n; aal5=n; pvc=n; svc=n; spvc=n; ec=n; mparty-3way=n;mparty-conference=n; lptime=10; hptime=20; silent-suppress-supp=n;rbk-on-conn-supp=n; isdn=n; dtmf=n; mf=n; fxo=n; fgd=n; mgcp-erqnt-unsupp=y;mgcp-hairpin-unsupp=y; mgcp-cmd-seq-unsupp=y; MGCP-NAS-UNSUPP=N;
``` |
| **Step 3** | Add the dial plan ID. |
| | ```
add dial-plan id=nasdp1; digit-string=214; reqd-digits=10; dest-id=destNAS;
``` |
| **Step 4** | Add the destination ID. |
| | ```
add destination dest-id=destNAS; call-type=NAS; route-type=None;
``` |
| **Step 5** | Provision the SS7 trunk groups. |
| | ```
add mgw id=c2421.192;tsap-addr=c2421.192.trnglab.cisco.com;call-agent-id=CA101;
mgw-profile-id=IAD2421;
``` |
Operator Services

The Operator Services feature allows routing of operator calls to a Feature Group D Operator Trunk (FGD OS) using the CAS MF Operator Package (MO). The following operator calls are included:

- 0-
- 0+
- 00
- 01+CC+NN
- 10XXXX + 0-
- 10XXXX + 0+
- 10XXXX + 00
- 10XXXX + 01+CC+NN

The operator call is routed to a CAS MO trunk group by sending the called number followed by information digits (I or II) and the calling number (ANI). All these digits are outpulsed to the CAS MO trunk group using multifrequency (MF) signaling. The information digits and ANI can be delivered in any one of these formats (configurable on a per terminating trunk basis):

- I + 7 digit ANI
- I + 10 digit ANI
- II + 7 digit ANI
- II + 10 digit ANI

Prerequisites

The Dial Plan table must be provisioned with a dial plan for operator calls.

An operator CAS MO terminating trunk group must be provisioned.

Supported Interfaces

Table 6-3 shows the interface support between call origination and termination.

<table>
<thead>
<tr>
<th></th>
<th>RGW termination</th>
<th>CAS termination</th>
<th>SS7 termination</th>
<th>ISDN termination</th>
<th>SIP termination</th>
</tr>
</thead>
<tbody>
<tr>
<td>RGW origination</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAS origination</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SS7 origination</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISDN origination</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SIP origination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Note: These calls can be terminated to another type of trunk group such as ISDN, SS7, and SIP, but in these cases the calls are treated as regular calls.

**Provisioning Operator Services**

To provision operator services, perform the following steps:

**Step 1**
Add the CAS trunk group profile and the operator trunk group.

```plaintext
add cas-tg-profile id=cas-OPS0; type=MO-10II; oss-sig=y; test-line=n;
```

```plaintext
add trunk-grp id=1500; tg-type=CAS; dial-plan-id=dpcas; sel-policy=LRU; 
direction=outgoing; glare=ODD; tg-profile-id=cas-OPS0; call-agent-id=CA166; status=oos;
```

**Step 2**
Add the operator trunk terminations to the Termination Prefix table.

```plaintext
add termination prefix=cas/ops/mo/; mgw-id=224.14:2434; type=TRUNK; mgcp-pkg-type=MO; 
port-start=1; port-end=24;
```

```plaintext
add trunk cic-start=5; cic-end=8; tgn-id=1500; termination-prefix=cas/ops/mo/; 
mgw-id=224.14:2434; termination-port-start=5; termination-port-end=8;
```

**Step 3**
Add the operator routes.

```plaintext
add route id=ops1500; tgn1-id=1500; lcr=y;
```

```plaintext
add route-guide id=ops1500; policy-type=route; policy-id=ops1500;
```

**Step 4**
Add the carrier ID and put the carrier in service.

```plaintext
add carrier id=0510; intra=y; intl=y; route-guide-id=ops1500; use-dial-plan=y;
```

```plaintext
change carrier id=0510; status=ins;
```

**Step 5**
Add the destination IDs.

```plaintext
add destination dest-id=ops-toll; call-type=toll; route-type=ROUTE; 
route-guide-id=ops1502; zero-plus=y;
```

```plaintext
add destination dest-id=ops-interlata; call-type=interlata; route-type=ROUTE; 
route-guide-id=ops1501; zero-plus=y;
```

```plaintext
add destination dest-id=ops-intl; call-type=intl; route-type=ROUTE; 
route-guide-id=ops1503; zero-plus=y;
```

```plaintext
add dial-plan id=dpcas; digit-string=817-313; reqd-digits=10; dest-id=ops-toll;
```

**Step 6**
Add the dial plan and international dial plan.

```plaintext
add dial-plan id=dpcas; digit-string=404-313; reqd-digits=10; dest-id=ops-interlata;
```

```plaintext
add int1-dial-plan cc=42; min-digits=6; max-digits=16; dest-id=ops-intl;
```
Originating Line Information Screening

The Originating Line Information (OLI) screening service provides screening based on the calling line info-digit.

Prerequisites

None.

Supported Interfaces

SS7, ISDN

Provisioning OLI

To provision OLI, perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Add the customer group.  
\[
\text{add cust-grp id=NONE-BLACK; overflow-carrier=0220; ani-wb-list=white; ii-restrict-list=BLACK;}
\] |
| Step 2 | Add the DN2 customer group digit string.  
\[
\text{add dn2cust-grp digit-string=800-919-2231; translated-dn=972-518-6588; carrier-id=0220; cust-grp-id=NONE-BLACK;}
\] |
| Step 3 | Add the ANI White/Black List customer group ID.  
\[
\text{add ani-wb-list cust-grp-id=NONE-BLACK; digit-string=972-518-3333;}
\] |
| Step 4 | Add the customer group.  
\[
\text{add cust-grp id=II; ii-restrict-list=black; add ii-restrict-list ii=29; cust-grp-id=NONE-BLACK;}
\] |

Note This step is for an incoming SS7 msg with OLI Screening.

| Step 5 | Add the ii-wb-list. This enables OLI screening.  
\[
\text{add ii-wb-list id=32; cos-restrict-id=cos-restrict-1;}
\] |
Outgoing Call Barring

The Outgoing Call Barring (OCB) feature is a superset of Class of Service (COS) screening and includes all the COS provisioning steps. However, COS functionality itself in OCB is optional, and need not be provisioned. OCB allows a subscriber to block certain types of outgoing calls from their phone, for example, all international or all long-distance can be blocked.

Prerequisites

None.

Supported Interfaces

Subscribers and trunks.

Provisioning OCB

This section describes how to provision OCB.

Note

The \textit{k-value} for subscriber in the Subscriber Feature Data table is automatically recorded by the system when a subscriber uses the Outgoing Call Barring Activate (OCBA) and Outgoing Call Barring Deactivate (OCBD) feature.

The \textit{count} and \textit{time} fields in the Subscriber Feature Data table are system internal. Do not manipulate.

Provisioning OCB

To provision OCB, perform the following steps:

\begin{enumerate}
\item Add the feature.

\begin{verbatim}
add feature fname=OCB; tdp1=COLLECTED_INFORMATION; tid1=cos-trigger; ttype1=R;
feature-server-id=FSPTC235; description=Outgoing Call Barring; grp-feature=N;
\end{verbatim}

\begin{verbatim}
add feature fname=OCBA; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R;
feature-server-id=FSPTC235; description=OCB Activation; grp-feature=N;
\end{verbatim}

\begin{verbatim}
add feature FNAME=OCBD; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R;
feature-server-id=FSPTC235; description=OCB Deactivation; grp-feature=N;
\end{verbatim}

\begin{verbatim}
add feature FNAME=OCBI; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R;
feature-server-id=FSPTC235; description=OCB Interrogation; grp-feature=N;
\end{verbatim}
\end{enumerate}
**Step 2**  Provision the COS feature.

*Note*  This step is optional and is required only under two circumstances:
- When COS screening functionality is required as a subset of OCB.
- The Black/White list screening functionality of OCB must be offered to a subscriber even if OCB is in a deactivated state.

**Step 3**  Provision the features into a service package.

```plaintext
add service id=1; fname1=OCB; fname2=OCBA; fname3=OCBD; fname4=OCBI;
```

**Step 4**  Add the VSCs.

```plaintext
add vsc fname=OCBA; digit-string=*54;
add vsc fname=OCBD; digit-string=#54;
add vsc fname=OCBI; digit-string=*#54;
```

**Step 5**  Provision a call type screening exception list. Enter as many call types (records) against OCB as required.

```plaintext
add nod-restrict-list fname=OCB; call-type=EMG;
```

**Step 6**  Provision the feature parameters if required.

```plaintext
change feature fname=OCB; pin-len=5; to=20; fail-cnt=4; lock-out=60;
```

**Step 7**  Add the service to the subscriber's service profile.

```plaintext
add subscriber-service-profile sub-id=sub1-plano.com; service-id=1;
```

*Note*  Further provisioning is by handset provisioning using feature activation and deactivations: Outgoing Call Barring Activate (OCBA) and Outgoing Call Barring Deactivate (OCBD).

**Step 8**  Add the subscriber's initial password.

```plaintext
add subscriber-feature-data sub-id=sub1-plano.com; fname=OCB; type1=PASSWD; value1=1234;
```

---

**Provisioning OCB for Centrex**

To provision OCB for Centrex, perform the following steps:

**Step 1**  Add the service to the subscriber's service profile.

```plaintext
add subscriber-service-profile sub-id=sub1-plano.com; service-id=1;
```

**Step 2**  Add the subscriber's initial password.

```plaintext
add subscriber-feature-data sub-id=sub1-plano.com; fname=OCB; type1=PASSWD; value1=1234;
```
Remote Activation of Call Forwarding and Pin Change

Step 3 Add the feature into the Custom Dial Plan table for the Centrex group.

```
add custom-dial-plan id=cdp1;digit-string=*54; nod=VSC;fname=OCBA;
cat-string=1111111111111111;
add custom-dial-plan id=cdp1;digit-string=#54; nod=VSC;fname=OCBD;
cat-string=1111111111111111;
add custom-dial-plan id=cdp1;digit-string=*#54; nod=VSC;fname=OCBI;
cat-string=1111111111111111;
```

Remote Activation of Call Forwarding and Pin Change

The Remote Call Forwarding Activation (RACF) feature allows a subscriber to remotely manipulate the Call Forwarding Unconditional (CFU) feature. A subscriber can always be reached regardless of its location and movements, provided RACF is provisioned and the subscriber has a RACF authorization code (a personal identification code, PIN). The PIN can be shared by a group, or can be unique to the individual subscriber.

**Note**
- RACF_PIN can only be assigned to those RACF subscribers who have unique pins.
- A unique pin is identified in the subscriber feature data entry for RACF as pintype-pin or pintype=newpin. The newpin type indicates that the subscriber has not yet changed their pin from the default pin assigned by the service provider. To use the RACF feature, a subscriber must first change their pin at least one from their home number. Once this is done, the pintype in the Subscriber Feature Data table is changed to PIN.
- If a subscriber has a non-unique pin, the subscriber cannot change it. It can only be changed through the CLI. For non-unique pin validation an authorization code must be provisioned and pintype must be set to authcode.
- Non-unique pins are typically assigned to a group of subscribers sharing the same pin.

Prerequisites

None.

Supported Interfaces

MGCP

Provisioning RACF

To provision RACF, perform the following steps.

**Note**
The Interactive Voice Response (IVR) DN value must be the same number as the IVR virtual subscriber. The number is used for RACF and Screen List Editing (SLE) activation features.
Step 1  Add the IVR DN to the Call Agent Configuration table. The IVR DN value must be the same number as the IVR virtual subscriber.

```
add ca-config type=IVR-DN; datatype=digits; value=9727892000;
```

Step 2  Add the IVR media server.

```
add mgw-profile id=ms-profile; vendor=cisco; silent-suppress-supp=n; rbk-on-conn-suppr
```

```p
packet-type=ip; aal1=n; aal2=n; aal5=n; svc=n; spvc=n; sec=n; mparty-conference=n; mparty-3way=n; num-per-mparty=1; num-of-mparty=1; lptime=10; hptime=10; spd=ntf=n; mf=y; fxs=n; fgd=n; backhaul-type=rudp; sdp-origfield-unsupp=y; sdp-sequence=unsupp=y; sdp-email-unsupp=y; sdp-telephone-unsupp=y; sdp-bandwidth-unsupp=y; sdp-info-unsupp=y; sdp-time=unsupp=y; sdp-attrib-unsupp=y; mgcp-erqnt=unsupp=y; mgcp-hairpin=unsupp=y; mgcp-qloop=unsupp=y; mgcp-3way=hsn shake=unsupp=y; mgcp-conn-id-at-gw=unsupp=n; mgcp-cmd-seq-unsupp=y; mgcp-vmwi=unsupp=y; termination-prefix=ann/;
```

```p
port-start=0; mgcpversion=mgcp-0-1; mgcp-payload=; mgcp-rsvp=unsupp=y;
```

```
add mgw id=ipunity-ms; tsap-addr=<ip addr of ms mgcp>; call-agent-id=ca166;
```

```p
gmw-profile-id=ms-profile; rgw=n; tgw=y; call-agent-control-port=0; ans=n; ivr=y; nas=n;
```

```p
pbx=n;
```

Step 3  Add the RACF Virtual Subscriber. All RACF subscribers call 972-789-8000 for remote access to call forwarding. Subscribers interact with the IVR subscriber when using the RACF PIN change feature.

```
add subscriber id=racf-annc-sub; category=racf; name=racf-annc-sub; status=active; dn1=972-789-8000; privacy=none; ring-type-dn1=1; tgn-id=1; usage-sens=n; sub-profile-id=sp; termin-type=route; policy-id=rt-annc;
```

Step 4  Define the internal IVR feature.

```
add feature fname=IVR; tdp1=T_ANSWER; tid1=T_ANSWER; ttype1=R; description=Internal IVR feature; feature-server-id=<feature server ID>;
```

Step 5  Define the RACF PIN change feature.

```
add feature fname=RACF_PIN; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R; tdp2=T_ANSWER; tid2=T_ANSWER; ttype2=R; description=RACF Pin Change; feature-server-id=<feature server id>;
```

Step 6  Assign the RACF service for subscribers with nonunique PINs. RACF-PIN is assigned to the IVR virtual subscriber.

```
add service id=RACF_SVC; fname1=RACF;
```

Step 7  Assign RACF and Pin Change service for subscribers with unique PINs.

```
add service id=RACF_N_PIN; fname1=RACF; fname2=RACF_PIN;
```

Step 8  Add the VSC for subscribers changing their PIN.

```
add vsc digit-string=*98; fname=RACF_PIN;
```
Provisioning RACF for a Subscriber

To provision RACF for a subscriber, perform the following steps:

Step 1  Assign the service to a subscriber. RACF is assigned only to a RACF virtual subscriber.
          add sub-service-profile; sub-id=racf-annc-sub; service-id=RACF_SVC;

Step 2  Assign the IVR feature to the RACF virtual subscriber. You can assign this service only to a RACF virtual subscriber.
          add sub-service-profile sub-id=racf_annc_sub; service-id=IVR_SVC;

Step 3  IVR feature is assigned to the IVR virtual subscriber. Only IVR virtual subscriber to have this service assigned.
          add sub-service-profile sub-id=ivr_annc_sub; service-id=IVR_SVC;

Step 4  Assign the RACF service to the subscriber. This step is for regular subscribers with RACF who have non-unique PINs, so an authorization code must be used. The RACF_PIN change feature is not assigned to this subscriber (sub1). If the subscriber has a unique pin, go to Step 5.
          add sub-service-profile sub-id=sub1; service-id=RACF_SVC;
          add subscriber-feature-data sub-id=sub1; fname=RACF; active=Y; type1=PINTYPE; value1=AUTHCODE;

Step 5  Assign the RACF Service to the subscriber. This subscriber (sub2) has a unique PIN. The pintype of newpin indicates that they must change it from their home/base phone, before they can use the RACF feature.
          add sub-service-profile sub-id=sub2; service-id=RACF_N_PIN;
          add subscriber-feature-data sub-id=sub2; fname=RACF; active=Y; type1=PINTYPE; value1=NEWPIN; type2=PIN; value2=99999;

Provisioning an Authorization Code

This section describes how to provision the Authorization Code Group and authorization code for subscribers with non-unique PINs.

Step 1  Add the authorization code group.
          add auth-code-grp id=DEFAULT_ACGROUP; description=authorization codes;

Step 2  Define the cos-restrict id for the authorization code group.
          add cos-restrict id=NO_RESTRICTION; casual-restrict-type=ALL-CICS-ALLOWED; national-restrict-type=ALL-NANP-CALLS; national-wb-list=NONE; intl-restrict-type=ALL-CC-ALLOWED; ii-restrict=NONE; block-900=N; block-976=N; block-da=N; block-nanp-oper-assist=N; block-intl-oper-assist=N; acct-code-allow=Y; acct-code-length=4; auth-code-allow=Y; auth-code-length=5; auth-code-grp-id=DEFAULT_ACGROUP;
Step 3  Add the authorization code for the authorization code group.

add auth-code auth-code-grp-id=DEFAULT_ACGROUP; id=12345; active=Y;

Note  This step sets auth-code 12345 as the PIN for RACF access by non-unique PIN subscribers.

Resource Reservation Protocol

The Resource Reservation Protocol (RSVP) feature allows a specific desired quality of service (QOS) to be reserved for the bearer path of a call.

Prerequisites

Provision the RSVP-UNSUPP=N field in the MGW Profile table.

Supported Interfaces

Not applicable

Provisioning the RSVP

To provision RSVP, perform the following step:

Step 1  Add RSVP to the Quality of Service table.

add_qos id=rsvp-pcmu;codec-type=g711u;rsvp-required=y;resource-reservation=g;

Screen List Editing

The Screen List Editing (SLE) feature allows subscribers to screen calls they do or do not wish put through using a list.

Prerequisites

None.

Supported Interfaces

Not applicable
Screen List Editing

Provisioning SLE

To offer SLE, which includes the features SCF, SCR, SCA and DRCW, with the ability for subscribers to provision them through IVR, perform the following steps:

**Note**

The IVR DN value must be the same number as the IVR virtual subscriber.

**Step 1**

Provision the Call Agent Configuration table.

```
add ca-config type=IVR-DN; datatype=string; value=9727892000;
add ca-config type=IVR-LIST-SIZE; datatype=integer; value=31;
add ca-config type=SLE-DE-THRESHOLD; datatype=integer; value=3;
add ca-config type=SLE-TO-THRESHOLD; datatype=integer; value=3;
add ca-config type=SLE-TIMER-T1; datatype=integer; value=4;
add ca-config type=SLE-TIMER-T2; datatype=integer; value=4;
add ca-config type=SLE-TIMER-T3; datatype=integer; value=4;
add ca-config type=SLE-TIMER-T4; datatype=integer; value=4;
add ca-config type=SLE-TIMER-T5; datatype=integer; value=3;
add ca-config type=SLE-TIMER-T6; datatype=integer; value=25;
add ca-config type=SLE-TIMER-T7; datatype=integer; value=4;
```

**Step 2**

Add the IVR media server.

```
add mgw-profile id=ms-profile; vendor=cisco; silent-suppress-supp=n; rbk-on-conn-supp=n;
packet-type=ip; aal1=n; aal2=n; aal5=n; pvc=n; svc=n; spvc=n;
ec=n; mparty-conference=n; mparty-3way=n; num-per-mparty=1; num-of-mparty=1;
lptime=10; hptime=10; isdn=n; dtmf=n; fxo=n; fxo=n; fgd=n;
backhaul-type=rudp; sdtp-origfield-unsupp=y; sdtp-sessname-unsupp=y; sdtp-email-unsupp=y;
sdp-unsupp=y; sdp-url-unsupp=y; sdp-bandwidth-unsupp=y; sdp-info-unsupp=y;
sdp-time-unsupp=y; sdp-attrb-unsupp=y; mgcp-erqnt-unsupp=y; mgcp-hairpin-unsupp=y;
mgcp-qloop-unsupp=y; mgcp-3way-hksake-unsupp=n; mgcp-conn-id-at-gw-unsupp=y;
mgcp-cmd-seq-unsupp=y; mgcp-vmwi-unsupp=y; termination-prefix=ann/;
port-start=0; mgcversion=mgcp-0-1; mgc-rsvp-unsupp=y;
```

```
add mgw id=ipunity-ms; tsap-addr=<ip addr of ms mgcp>; call-agent-id=ca166;
mgw-profile-id=ms-profile; rgw=n; tgw=y; call-agent-control-port=0; ans=n;ivr=y; nas=n;
pbx=n;
```

**Step 3**

Add the IVR trunks.

```
add annc-tg-profile id=annc_tg_p; annc=N; ivr=Y; auto_answer=Y;
add termination prefix=ann/; port-start=0; port-end=30; type=trunk; mgw-id=ipunity_ms;
add trunk-grp id=1; call-agent-id=CA146; mgw-id=ipunity_ms;
```

```
tg-profile-id=annc_tg_p; mgcp-pkg-type=audio;
add trunk cic-start=1; cic-end=30; tg-name=1 termination prefix=ann/;
termination-port-start=0; termination-port-end=29; mgw-id=ipunity_ms;
```
Chapter 6  Provisioning Features and Services

Screen List Editing

Step 4  Add the IVR virtual subscriber.

```
add ndc digit-string=972;
add exchange-code ndc=972; ec=789;
add office-code ndc=972; ec=789; dn-group=xxxx; call-agent-id=CA146;
add destination dest-id=ivr; call-type=LOCAL; route-type=sub;
add dial-plan id=dp; digit-string=972-789; reqd-digits=10; dest-id=ivr
add pop id=1; state=tx; country=usa; timezone=CST;
add subscriber-profile id=sp; dial-plan-id=dp; pop-id=1;
add route id=rt_annnc; tgn1-id=1; tg-selection=LCR;
add subscriber ID=ivr_annnc_sub; CATEGORY=IVR; NAME=ivr_annnc_sub; STATUS=ACTIVE;
dn1=972-789-2000; PRIVACY=NONE; RING-TYPE-DN1=1; TGN-ID=1; USAGE-SENS=N;
SUB-PROFILE-ID=sp; TERM-TYPE=ROUTE; POLICY-ID=rt_annnc;
```

change trunk_grp id=1; call-agent-id=CA146; main-sub-id=ivr_annnc_sub;
add route-guide id=rg_annnc; policy-type=ROUTE; policy-id=rt_annnc;

Step 5  Define the SCR feature.

```
add feature fname=SCF; tdp1=TERMINATION_ATTEMPT_AUTHORIZED;
tid1=TERMINATION_ATTEMPT_AUTHORIZED; ttype1=R; description=Selective Call Forwarding;
feature-server-id=<feature server ID>;
```

Step 6  Define the SCF Activation feature.

```
add feature fname=SCF_ACT; tdp1=COLLECTED_INFORMATION;
tid1=VERTICAL_SERVICE_CODE;ttype1=R; description=Selective Call Fwd Activation;
feature-server-id=<feature server ID>;
```

Step 7  Define the SCR feature.

```
add feature fname=SCR; tdp1=TERMINATION_ATTEMPT_AUTHORIZED;
tid1=TERMINATION_ATTEMPT_AUTHORIZED; ttype1=R; description=Selective Call Rejection;
feature-server-id=<feature server ID>;
```

Step 8  Define the SCR Activation feature.

```
add feature fname=SCR_ACT; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE;
ttype1=R; description=Selective Call Rejection Act; feature-server-id=<feature server ID>;
```

Step 9  Define the SCA feature.

```
add feature fname=SCA;tdp1=TERMINATION_ATTEMPT_AUTHORIZED;
tid1=TERMINATION_ATTEMPT_AUTHORIZED;ttype1=R; description=Selective Call Acceptance;
feature-server-id=<feature server ID>;
```

Step 10  Define the SCA Activation feature.

```
add feature fname=SCA_ACT; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE;
ttype1=R; description=Selective Call Acceptance Act; feature-server-id=<feature server ID>;
```

Step 11  Define the DRCW feature.

```
add feature fname=DRCW;tdp1=TERMINATION_ATTEMPT_AUTHORIZED;
tid1=TERMINATION_ATTEMPT_AUTHORIZED;ttype1=R;description=Distinctive Ring CW;
feature-server-id=<feature server ID>;
```

Step 12  Define the DRCW Activation feature.

```
add feature fname=DRCW_ACT; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE;
ttype1=R; description=Distinctive Ring CW Act; feature-server-id=<feature server ID>;
```

Step 13  Define the Internal IVR feature.

```
add feature fname=IVR; tdp1=T_ANSWER; tid1=T_ANSWER; ttype1=R; description=Internal IVR
feature; feature-server-id=<feature server ID>;
```
Provisioning SLE for Subscribers, Centrex, and MLHG

To provision SLE for subscribers, Centrex, or MLHG, perform the following steps:

**Step 1**
Add SLE activation features to the IVR virtual subscriber. Only these features and RACF_PIN can be assigned to this subscriber.

```
add sub-service-profile sub-id=ivr-annc-sub; service-id=IVR_SVC;
```

**Step 2**
Add the SLE features to a local subscriber.

```
add sub-service-profile sub-id=sub1; service-id=1;
```

Provisioning SCF, SCR, SCA and DRCW — Alternative Method

This section describes an alternation method for provisioning the SCF, SCR, SCA and DRCW features. The steps are similar for all; DRCW is used in the following example steps.

**Note**
DRCW subscribers require CW, CIDCW, or CWD for the call waiting portion of DRCW to work.

**Step 1**
Add the service for the chosen feature.

```
add service id=10;fname1=DRCW;
```

**Step 2**
Add the service to the local subscriber.

```
add sub-service-profile sub-id=sub1; service-id=10;
```

**Step 3**
Activate/Deactivate feature in the Subscriber Feature Data table.

```
Add sub-feature-data sub-id=sub1; fname=DRCW; Active=Y (or N);
```
Provisioning Features and Services

Selective Call Acceptance

The Selective Call Acceptance (SCA) service allows a subscriber to only accept call attempts from a limited number of calling parties. To use the service, the subscriber specifies the DNs of calls to be accepted.

Prerequisites

The media server database must be set up.

Supported Interfaces

MGCP

Provisioning SCA

To provision SCA, perform the following steps:

Step 1 Define the SCA feature.

```
add feature fname=SCA; tdpl=TERMINATION_ATTEMPT_AUTHORIZED;
tid1=TERMINATION_ATTEMPT_AUTHORIZED; ttype1=R; feature-server-id=FSPTC235;
description=Selective Call Acceptance;
```

Step 2 Add the service ID.

```
add service id=54; fname1=SCA; fname2=SCA_ACT; description=Common for all subscribers;
```

Step 3 Add the VSC digit string.

```
add vsc digit-string=*64; fname=SCA_ACT;
add vsc digit-string=*84; fname=SCA_ACT;
```

Step 4 Add the feature associated DN to the subscriber SLE table.

\[\text{Note}\]
To add multiple DNs for a feature make additional entries with the same feature name, but different DNs.

- For features SCR, SCA and DRCW, add the SLE subscriber.
  ```
  add sle sub-id=sub1; fname=DRCW; dn=9726712355;
  ```
- For SCF, change the Subscriber Feature Data table to define the forward-to number.
  ```
  change sub-feature-data sub-id=sub1; fname=SCF; type1=FDN1; value1=469-575-4567;
  ```
**Selective Call Forwarding**

The Selective Call Forwarding (SCF) service allows a subscriber to forward call attempts from a limited number of calling parties. To use the service, the subscriber specifies the DNs of calls to be forwarded to the forwarding DN (FDN).

**Prerequisites**

Media server database must be set up.

**Supported Interfaces**

MGCP

**Provisioning SCF**

To provision SCF, perform the following steps:

**Step 1** Define the SCF feature.

```
add feature fname=SCF; tdp1=TERMINATION_ATTEMPT_AUTHORIZED;
tid1=TERMINATION_ATTEMPT_AUTHORIZED; ttype1=R; feature-server-id=FSPTC235;
description=Selective Call Forwarding;
```

**Step 2** Add the service ID.

```
add service id=53; fname1=SCF; fname2=SCF_ACT; description=Common for all subscribers;
```

**Step 3** Add the VSC digit strings.

```
add vsc digit-string=*63; fname=SCF_ACT;
add vsc digit-string=*83; fname=SCF_ACT;
```
Selective Call Reject

The Selective Call Reject (SCR) service enables you to instruct the Telephone System to reject call attempts from a limited number of calling parties to your line. To use the service, you can specify directory numbers (DNs) of calling parties applicable for rejection.

Prerequisites

Media server database must be set up

Supported Interfaces

MGCP

Provisioning SCR

To provision SCR, perform the following steps:

Step 1 Define the SCR feature.

add feature fname=SCR; tdp=TERMINATION_ATTEMPT_AUTHORIZED; tid=TERMINATION_ATTEMPT_AUTHORIZED; ttype=R; feature-server-id=FSPTC235; DESCRIPTION=Selective Call Rejection;
Service Code 311: Non Emergency Service

To provision SCR for Centrex subscribers, perform the following step:

Step 1  Add the CDP ID.

add cdp id=cdp1; digit-string=*60; nod=VSC; FNAME=SCR_ACT; cat-string=1111111111111111;
add cdp id=cdp1; digit-string=*80; nod=VSC; FNAME=SCR_ACT; cat-string=1111111111111111;

Prerequisites

The Dial Plan table must be provisioned with a dial plan for 311 non-emergency calls. An operator CAS MO terminating trunk group must be provisioned.
Supported Interfaces

Table 6-4 shows the interface support between call origination and termination.

<table>
<thead>
<tr>
<th></th>
<th>RGW termination</th>
<th>CAS termination</th>
<th>SS7 termination</th>
<th>ISDN termination</th>
<th>SIP termination</th>
</tr>
</thead>
<tbody>
<tr>
<td>RGW origination</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAS origination</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SS7 origination</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note**
These calls can also be terminated to another type of trunk group such as ISDN, SS7, and SIP, but in these cases the calls are treated as regular calls.

Provisioning Service Code 311: NES

To provision Service Code 311: NES, perform the following steps:

**Step 1**
Add the operator trunk groups.
```
add cas-tg-profile id=cas-OPS0; type=MO-10II; oss-sig=y; test-line=n;
add trunk-grp id=1500; tg-type=CAS; dial-plan-id=dpcas; sel-policy=LRU; direction=BOTH;
glare=ODD; tg-profile-id=cas-OPS0; call-agent-id=CA166; status=oos;
```

**Step 2**
Add the operator trunk terminations.
```
add termination prefix=cas/ops/mo/; mgw-id=224.14:2434; type=TRUNK; mgcp-pkg-type=MO;
port-start=1; port-end=24;
add trunk cic-start=5; cic-end=8; tgn-id=1500; termination-prefix=cas/ops/mo/;
mgw-id=224.14:2434; termination-port-start=5; termination-port-end=8;
```

**Step 3**
Add the operator routes and route guide ID.
```
add route id=ops1500; tgn1-id=1500; lcr=y;
add route-guide id=ops1500; policy-type=route; policy-id=ops1500;
```

**Step 4**
Add the Destination and Service Code 311: NES dial plan.
```
add destination dest-id=ops311; call-type=non-emg; route-type=ROUTE;
route-guide-id=ops1500; zero-pluss=y;
add dial-plan id=dpcas; digit-string=311; dest-id=ops311; reqd-digits=3;
```
Service Code 411: Directory Assistance

The Service Code 411: Directory Assistance (DA) feature processes and routes 411 DA calls to a CAS MO (FGD OS) trunk group. Using MF signaling, the called party number (411), the information digits, and the ANI are delivered to the CAS MO trunk group. A billing record is generated indicating that this is a 411 DA call.

The information digits and ANI can be delivered in any one of these formats (configurable on a per terminating trunk basis):

- I + 7 digit ANI
- I + 10 digit ANI
- II + 7 digit ANI
- II + 10 digit ANI

Prerequisites

The dial-plan table must be provisioned with a DA Dial Plan ((0/1) + 411, (10XXXXX) + (0/1) + NPA + 555 + 1212).

An operator CAS MO terminating trunk group must be provisioned.

Supported Interfaces

Table 6-5 shows the interface support between call origination and termination.

<table>
<thead>
<tr>
<th></th>
<th>RGW termination</th>
<th>CAS termination</th>
<th>SS7 termination</th>
<th>ISDN termination</th>
<th>SIP termination</th>
</tr>
</thead>
<tbody>
<tr>
<td>RGW origination</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAS origination</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SS7 origination</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISDN origination</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SIP origination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Note

These calls can also be terminated to another type of trunk group such as ISDN, SS7, and SIP, but in these cases the calls are treated as regular calls.
Provisioning Service Code 411: DA

To provision Service Code 411: DA, perform the following steps:

**Step 1** Add the operator trunk group.
```
add cas-tg-profile id=cas-OPS0; type=MO-10II; oss-sig=y; test-line=n;
add trunk-grp id=1500; tg-type=CAS; dial-plan-id=dpcas; sel-policy=LRU; direction=BOTH; glare=ODD; tg-profile-id=cas-OPS0; call-agent-id=CA166; status=ooos;
```

**Step 2** Add the operator trunk terminations.
```
add termination prefix=cas/ops/mo/; mgw-id=224.14:2434; type=TRUNK; mgcp-pkg-type=MO; port-start=1; port-end=24;
add trunk cic-start=5; cic-end=8; tgn-id=1500; termination-prefix=cas/ops/mo/; mgw-id=224.14:2434; termination-port-start=5; termination-port-end=8;
```

**Step 3** Add the operator routes and route guide ID.
```
add route id=ops1500; tgn1-id=1500; lcr=y;
add route-guide id=ops1500; policy-type=route; policy-id=ops1500;
```

**Step 4** Add the destinations for Service Code 411: DA.
```
add destination dest-id=ops411; call-type=da; route-type=ROUTE; route-guide-id=ops1500; zero-plus=y;
add destination dest-id=ops1411; call-type=da-toll; route-type=ROUTE; route-guide-id=ops1500; zero-plus=y;
```

**Step 5** Add the dial plan for Service Code 411: DA.
```
add dial-plan id=dpcas; digit-string=411; dest-id=ops1411; reqd-digits=3;
```

Service Code 611: Repair

The Service Code 611: Repair feature processes and routes 611 repair calls to a CAS MO (FGD OS) trunk group. Using MF signaling, the called party number (611), the information digits, and the ANI are delivered to the CAS MO trunk group. A billing record is generated indicating that this is a 611 Repair service call.

The information digits and ANI can be delivered in any one of these formats (configurable on a per terminating trunk basis):
- I + 7 digit ANI
- I + 10 digit ANI
- II + 7 digit ANI
- II + 10 digit ANI
Service Code 611: Repair

Prerequisites

The Dial Plan table must be provisioned with a Service Code 611: Repair Dial Plan. An operator CAS MO terminating trunk group must be provisioned.

Supported Interfaces

Table 6-6 shows the interface support between call origination and termination.

<table>
<thead>
<tr>
<th>Service Code 611, Repair Service Supported Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>RGW termination</td>
</tr>
<tr>
<td>RGW origination</td>
</tr>
<tr>
<td>CAS origination</td>
</tr>
<tr>
<td>SS7 origination</td>
</tr>
<tr>
<td>ISDN origination</td>
</tr>
<tr>
<td>SIP origination</td>
</tr>
</tbody>
</table>

Note

These calls can also be terminated to another type of trunk group such as ISDN, SS7, and SIP, but in these cases the calls are treated as regular calls.

Provisioning Service Code 611: Repair

To provision Service Code 611: Repair, perform the following steps:

Step 1
Add the operator trunk groups.

add cas-tg-profile id=cas-OPS0; type=MO-10II; oss-sig=y; test-line=n;
add trunk-grp id=1500; tgn-type=CAS; dial-plan-id=dpcas; sel-policy=LRU; direction=BOTH; glare=ODD; tgn-profile-id=cas-OPS0; call-agent-id=CA166; status=oos;

Step 2
Add the operator trunk terminations.

add termination prefix=cas/ops/mo/; mgw-id=224.14:2434; type=TRUNK; mgcp-pkg-type=MO; port-start=1; port-end=24;
add trunk cic-start=5; cic-end=8; tgn-id=1500; termination-prefix=cas/ops/mo/; mgw-id=224.14:2434; termination-port-start=5; termination-port-end=8;

Step 3
Add the operator routes and route guide ID.

add route id=ops1500; tgn1-id=1500; lcr=y;
add route-guide id=ops1500; policy-type=route; policy-id=ops1500;
Step 4  Add the destination.

```
add destination dest-id=ops611; call-type=repair; route-type=ROUTE;
route-guide-id=ops1500; zero-plus=y;
```

Step 5  Add the dial plan ID.

```
add dial-plan id=dpcas; digit-string=611; dest-id=ops611; reqd-digits=3;
```

Service Code 711: Telecommunications Devices for the Deaf Relay

The Service Code 711: Telecommunications Devices for the Deaf (TDD) Relay feature processes and routes 711 TDD relay calls to a CAS MO (FGD OS) trunk group. Using MF signaling, the called party number (711), the information digits, and the ANI are delivered to the CAS MO trunk group. A billing record is generated indicating that this is a 711 TDD Relay call.

The information digits and ANI can be delivered in any one of these formats (configurable on a per terminating trunk basis):

- I + 7 digit ANI
- I + 10 digit ANI
- II + 7 digit ANI
- II + 10 digit ANI

Prerequisites

The Dial Plan table be provisioned with a dial plan for 711 TDD relay calls.

An operator CAS MO terminating trunk group must be provisioned.

Supported Interfaces

Table 6-7 shows the interface support between call origination and termination.

<table>
<thead>
<tr>
<th></th>
<th>RGW termination</th>
<th>CAS termination</th>
<th>SS7 termination</th>
<th>ISDN termination</th>
<th>SIP termination</th>
</tr>
</thead>
<tbody>
<tr>
<td>RGW origination</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAS origination</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SS7 origination</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 6      Provisioning Features and Services

Service Code 711: Telecommunications Devices for the Deaf Relay

Table 6-7   Service Code 711, TDD Relay Supported Interfaces

<table>
<thead>
<tr>
<th>RGW termination</th>
<th>CAS termination</th>
<th>SS7 termination</th>
<th>ISDN termination</th>
<th>SIP termination</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISDN origination</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP origination</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: These calls can also be terminated to another type of trunk group such as ISDN, SS7, and SIP, but in these cases the calls are treated as regular calls.

Provisioning Service Code 711: TDD Relay

To provision Service Code 711: TDD Relay, perform the following steps:

Step 1  Add the operator trunk group.

```
add cas-tg-profile id=cas-OPS0; type=MO-10II; oss-sig=y; test-line=n;
```

```
add trunk-grp id=1500; tg-type=CAS; dial-plan-id=dpcas; sel-policy=LRU; direction=BOTH; glare=ODD; tg-profile-id=cas-OPS0; call-agent-id=CA166; status=oos;
```

Step 2  Add the operator trunk terminations.

```
add termination prefix=cas/ops/mo/; mgw-id=224.14:2434; type=TRUNK; mgcp-pkg-type=MO; port-start=1; port-end=24;
```

```
add trunk cic-start=5; cic-end=8; tgn-id=1500; termination-prefix=cas/ops/mo/; mgw-id=224.14:2434; termination-port-start=5; termination-port-end=8;
```

Step 3  Add the operator routes and route guide ID.

```
add route id=ops1500; tgn1-id=1500; lcr=y;
```

```
add route-guide id=ops1500; policy-type=route; policy-id=ops1500;
```

Step 4  Add the destination ID.

```
add destination dest-id=ops711; call-type=relay; route-type=ROUTE; route-guide-id=ops1500; zero-plus=y;
```

Step 5  Add the dial plan.

```
add dial-plan id=dpcas; digit-string=711; dest-id=ops711; reqd-digits=3;
```
Service Code 811: Telco Business Office

The Service Code 811: Telco Business Office feature processes and routes Service Code 811 Telco Business Office calls to a CAS MO (FGD OS) trunk group. Using MF signaling, the called party number (811), the information digits, and the ANI are delivered to the CAS MO trunk group. A billing record is generated indicating that this is a Service Code 811 Telco Business Office service call.

The information digits and ANI can be delivered in any one of these formats (configurable on a per terminating trunk basis):
- I + 7 digit ANI
- I + 10 digit ANI
- II + 7 digit ANI
- II + 10 digit ANI

Prerequisites

The Dial Plan table must be provisioned with a dial plan for 811 Telco Business Office calls.

An operator CAS MO terminating trunk group must be provisioned.

Supported Interfaces

Table 6-8 shows the interface support between call origination and termination.

<table>
<thead>
<tr>
<th></th>
<th>RGW termination</th>
<th>CAS termination</th>
<th>SS7 termination</th>
<th>ISDN termination</th>
<th>SIP termination</th>
</tr>
</thead>
<tbody>
<tr>
<td>RGW origination</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAS origination</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SS7 origination</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISDN origination</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SIP origination</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Provisioning Service Code 811: Telco Business Office

To provision Service Code 811: Telco Business Office, perform the following steps:

**Step 1** Add the operator trunk group.
```
add cas-tg-profile id=cas-OPS0; type=MO-10II; oss-sig=y; test-line=n;
```
```
add trunk-grp id=1500; tg-type=CAS; dial-plan-id=dpcas; sel-policy=LRU; direction=BOTH;
glare=ODD; tg-profile-id=cas-OPS0; call-agent-id=CA166; status=ois;
```

**Step 2** Add the operator trunk terminations.
```
add termination prefix=cas/ops/mo/; mgw-id=224.14:2434; type=TRUNK; mgcp-pkg-type=MO;
port-start=1; port-end=24;
```
```
add trunk cic-start=5; cic-end=8; tgn-id=1500; termination-prefix=cas/ops/mo/;
mgw-id=224.14:2434; termination-port-start=5; termination-port-end=8;
```

**Step 3** Add the operator routes and route guide ID.
```
add route id=ops1500; tgn1-id=1500; lcr=y;
```
```
add route-guide id=ops1500; policy-type=route; policy-id=ops1500;
```

**Step 4** Add the destination.
```
add destination dest-id=ops811; call-type=business; route-type=ROUTE;
route-guide-id=ops1500; zero-plus=y;
```

**Step 5** Add the dial plan.
```
add dial-plan id=dpcas; digit-string=811; dest-id=ops811; reqd-digits=3;
```

Service Code 911: Emergency

The Service Code 911: Emergency feature processes and routes both basic and enhanced 911 emergency calls to a CAS MO (FGD OS) trunk group. A billing record is generated upon termination of the call indicating that this is a 911 emergency call. The following capabilities are implemented with this feature:

- Information digits and ANI delivery
- Optional 911 called party hold
- 911 recall function
- 911 recall function during conversation
- Priority over other call processing features (call waiting, three way calling, etc. are disabled during 911 calls)
- The information digits and ANI can be delivered in any one of these formats (configurable on a per terminating trunk basis) using MF signaling:
  - 1 + 7 digit ANI
  - 1 + 10 digit ANI
  - II + 7 digit ANI
  - II + 10 digit ANI
With the ANI delivery options shown above, and the option of called party hold, both Basic 911 service and Enhanced 911 service (end office) are fully supported.

**Prerequisites**

The Dial Plan table must be provisioned with a 911 dial plan.

A 911 CAS MO terminating trunk group must be provisioned.

For Centrex Provisioning

1. POTS access for a Centrex group must be provisioned.
2. A digit map for the emergency number must be provisioned in the Call Agent (for example: 911 for NANP).

**Supported Interfaces**

Table 6-9 shows the interface support between call origination and termination.

<table>
<thead>
<tr>
<th></th>
<th>RGW termination</th>
<th>CAS termination</th>
<th>SS7 termination</th>
<th>ISDN termination</th>
<th>SIP termination</th>
</tr>
</thead>
<tbody>
<tr>
<td>RGW origination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAS origination</td>
<td></td>
<td>X*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SS7 origination</td>
<td></td>
<td></td>
<td>X*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISDN origination</td>
<td></td>
<td></td>
<td></td>
<td>X*</td>
<td></td>
</tr>
<tr>
<td>SIP origination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X*</td>
</tr>
</tbody>
</table>

**Note**
The 911 features of called party hold and 911 recall are not applicable for these originations.

**Note**
These calls can also be terminated to another type of trunk group such as ISDN, SS7, and SIP, but in these cases the calls are treated as regular calls.
Provisioning Service Code 911: Emergency

To provision Service Code 911: Emergency, perform the following steps:

**Step 1** Add the feature.
```
add feature; fname=911; tdp1=COLLECTED_INFORMATION; tid1=911_TRIGGER; ttype1=R;
description=Emergency Service; feature_server_id=FSPTC325;
```

**Step 2** Change the Call Agent Configuration table entry for the default office service id if the entry is different from the entry in the Call Agent Configuration Base table.
```
change ca-config type=DEFAULT-OFFICE-SERVICE-ID; datatype=integer; value=469;
```

**Step 3** Change the Call Agent Configuration table entry for called party hold control as per your network requirements.
```
change ca-config type=E911-CALLED-PARTY-HOLD; datatype=boolean; value=Y;
```

**Step 4** Add the service.
```
add service; service-id=469; fname=911;
```

---

Provisioning 911 Emergency Services for Centrex

The following tasks are required when provisioning 911 emergency services for Centrex subscribers:

1. POTS access for the Centrex group must be provisioned.
2. The Call Agent must be provisioned with a digit-map for the emergency number (for example: 911 for NANP).

---

Speed Dialing

The Speed Dialing feature allows a subscriber to assign either a one-digit or two-digit abbreviated code to frequently called numbers. One-digit speed dialing accommodates up to eight numbers (2 through 9) for POTS and BBG customers, while two-digit speed dialing accommodates up to thirty numbers (20 through 49) for long distance, local, international or emergency numbers.

---

Prerequisites

- Office default database must be set up
- Subscriber Centrex must be set up
- MLHG Centrex-MLHG provisioning must be completed
- Speed dialing provisioning must be completed
- Speed dialing group provisioning must be completed
Supported Interfaces

Not applicable

Provisioning Speed Dialing

To provision speed dialing, perform the following steps:

**Step 1**  Define the feature.

```plaintext
add feature fname=SC1D_ACT; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R; description=One Digit Speed Call Activation; feature-server-id=FSPTC235;

add feature fname=SC2D_ACT; tdp1=COLLECTED_INFORMATION; tid1=VERTICAL_SERVICE_CODE; ttype1=R; description=Two Digit Speed Call Activation; feature-server-id=FSPTC235;

add feature fname=GSC1D; tdp1=COLLECTED_INFORMATION; tid1=SC1D_TRIGGER; ttype1=R; description=Group One Digit Speed Call; feature-server-id=FSPTC235; GRP-FEATURE=Y

add feature fname=GSC2D; tdp1=COLLECTED_INFORMATION; tid1=SC2D_TRIGGER; ttype1=R; description=Group Two Digit Speed Call; feature-server-id=FSPTC235; GRP-FEATURE=Y;

add feature fname=SC1D; tdp1=COLLECTED_INFORMATION; tid1=SC1D_TRIGGER; ttype1=R; description=One Digit Speed Call; feature-server-id=FSPTC235;

add feature fname=SC2D; tdp1=COLLECTED_INFORMATION; tid1=SC2D_TRIGGER; ttype1=R; description=Two Digit Speed Call; feature-server-id=FSPTC235;
```

**Step 2**  Add the VSCs.

```plaintext
add vsc digit-string=*74; fname=SC1D_ACT;
add vsc digit-string=*75; fname=SC2D_ACT;
```

**Step 3**  Add the feature service IDs.

```plaintext
add service id=498; fname1=SC1D_ACT; fname2=SC1D;
add service id=499; fname1=SC2D_ACT; fname2=SC2D;
add service id=500; fname1=GSC1D;
add service id=501; fname1=GSC2D;
```

**Step 4**  Add the service ID to the subscribers.

```plaintext
add sub-service-profile sub-id=127-5; service-id=498;
add sub-service-profile sub-id=127-6; service-id=499;
add sub-service-profile sub-id=127-1; service-id=500;
add sub-service-profile sub-id=127-1; service-id=501;
```

**Step 5**  Change the digit map and add the digit pattern so speed dialing can be invoked.

```plaintext

```

Provisioning Speed Dialing for Subscribers and MLHGs

To provision speed dialing for subscribers and MLHGs, perform the following step:

Step 1 Add the service to the subscriber.
```
add sub-service-profile sub-id=sub-1-4;service-id=499;priority=4;
```

Provisioning Speed Dialing for Centrex

To provision speed dialing for Centrex, perform the following steps:

Step 1 Add the service to the subscriber.
```
add sub-service-profile sub-id=sub-1-4;service-id=499;priority=4;
```

Step 2 Add the service to the Custom Dial Plan table.
```
add custom-dial-plan id=cdp1;digit-string=*74;nod=vsc;fname=SC1D_ACT;
cat-string=1111111111111111;
```
Split Numbering Plan Area

The Split Numbering Plan Area (NPA) feature converts a specific NPA or NPA-NXX to a new NPA. This feature was designed to facilitate the operation of dividing an area served by one NPA into smaller areas served by different NPAs (such as when an area is running out of telephone numbers based on a particular NPA, and new NPAs are introduced).

For the Split NPA procedure to be initiated, a permissive period is first established. During this period, the numbers that are scheduled to be served by a new NPA can be reached using both the old NPA and the new NPA. Once the permissive period ends, these numbers are then reached only using the new NPA. When these numbers cannot be reached using the old NPA, the old NPA dialing plan becomes vacant and available for assignment to different subscribers.
Table 6-10 provides an overview of the Split NPA provisioning steps.

Table 6-10  Split NPA Provisioning Overview

1. Create a Split NPA command entry for each NPA-NXX that needs to be converted (if a NXX is not defined, the whole NPA range is converted).
2. Duplicate all the numbers with old NPA-NXX and new NPA-NXX. This is executed as a single command step, and must be done before the permissive period starts.
3. Update the ANI records for all the new NPA-NXX numbers (the calling number now becomes the new NPA-NXX number in operations such a Calling Number Delivery). This is executed as a single command step, and must be done during the permissive period.
4. Clean up the old NPA-NXX numbers (these numbers become vacant numbers, and are available to be assigned to new subscribers if necessary). This is executed as a single command step, and must be done after the permissive period ends.

Prerequisites

The data for the old NPA-NXX (subscriber tables, dial-plan tables, and so forth) must already be provisioned prior provisioning a Split NPA.

Supported Interfaces

Table 6-11 shows the interface support between call origination and termination.

Table 6-11  Split NPA Supported Interfaces

<table>
<thead>
<tr>
<th></th>
<th>RGW termination</th>
<th>CAS termination</th>
<th>SS7 termination</th>
<th>ISDN termination</th>
<th>SIP termination</th>
</tr>
</thead>
<tbody>
<tr>
<td>RGW origination</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>CAS origination</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SS7 origination</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>ISDN origination</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SIP origination</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Provisioning a Split NPA

To provision a split NPA, perform the following steps:

**Step 1** Define the old split NPA.

```
add split-npa old-npa=214-671; new-npa=972-671; start-date=2001-01-30; end-date=2001-02-26;
```

```
add split-npa old-npa=215; new-npa=973; start-date=2001-01-30; end-date=2001-02-26;
```

**Step 2** Verify the status of the split NPA.

```
show split-npa old-npa=214-671
show split-npa old-npa=214%
show split-npa old-npa=214;
show split-npa old-npa=215;
```

**Step 3** Create duplicate records of the old and new NPAs.

```
change split-npa old-npa=214-671; dup-records=y;
change split-npa old-npa=215; dup-records=y;
```

**Step 4** Verify the old split NPAs.

```
show split-npa old-npa=214-671
show split-npa old-npa=215;
```

**Step 5** Update the ANI so that the new NPA is used.

```
change split-npa old-npa=214-671; update-ani=y;
change split-npa old-npa=215; update-ani=y;
```

**Step 6** Verify the old split NPA.

```
show split-npa old-npa=214-671
show split-npa old-npa=215;
```

**Step 7** Delete the old NPA records.

```
change split-npa old-npa=214-671; cleanup=y;
change split-npa old-npa=215; cleanup=y;
```

**Step 8** Verify the old split NPA.

```
show split-npa old-npa=214-671
show split-npa old-npa=215;
```
T.38 Fax Relay

The T.38 Fax Relay feature provides standards-based fax relay protocol support on Cisco 3600 series, and Cisco MC3810 series and C5850 multiservice gateways. The Cisco proprietary fax relay solution is sometimes not an ideal solution for enterprise and service provider customers who have implemented a mixed vendor network. Because the T.38 Fax Relay protocol is standards based, Cisco gateways and gatekeepers will now be able to interoperate with third-party T.38-enabled gateways and gatekeepers in a mixed vendor network where realtime fax relay capabilities are required.

Table 6-12 shows the different fax configuration types.

<table>
<thead>
<tr>
<th>Fax Type</th>
<th>CA (MGW profile)</th>
<th>MGCP (GW profile)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Passthru</strong></td>
<td>FAX-INBAND=y</td>
<td>#mgcp modem passthrough VOIP mode NSE</td>
</tr>
<tr>
<td>Using a Cisco proprietary modem—passthru NSE</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>T.38 Relay</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• t38 (CA controlled) mgcp preferred</td>
<td>FAX-CA mode=y</td>
<td>#mgcp package fxr-package</td>
</tr>
<tr>
<td>• t38 (GW controlled) proprietary</td>
<td>FAX-GW mode=y</td>
<td>#mgcp fax t38</td>
</tr>
<tr>
<td><strong>QoS</strong>—fax preferred mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• MGW/IOS pref=gw controlled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note* An MGCP to MGCP T38 CA configuration requires an MGW configuration.

**Prerequisites**

None.

**Supported Interfaces**

Not applicable
Provisioning T.38 Fax Relay

To provision T.38 Fax Relay for an MGCP-to-MGCP scenario, perform the following step:

**Step 1**
Add T.38 Fax Relay to the MGW Profile.
```
change mgw-profile id=XXX; fax-t38-gwmode-suppy; fax-t38-camode-supp=n;
fax-pref-mode=fax-t38-gwmode;
```

Three-Way Calling

The Three-Way Calling (TWC) service permits three people at three different locations to talk together at the same time. Regardless of who receives the initial call, anyone can use TWC to add a third person to the call. The call can be continued if either of the other parties hangs up. However, when the subscriber who initiated TWC hangs up, the other parties are automatically disconnected because the subscriber who initiated TWC controls the service. Once TWC is initiated, all the parties in the call can simultaneously hear the other parties.

**Prerequisites**

None.

**Supported Interfaces**

Not applicable

Provisioning TWC

To provision TWC, perform the following step:

**Step 1**
Define the TWC feature.
```
add feature fname=TWC; TDP1=O_MID_CALL; tid1=O_SWITCH_HOOK_FLASH_IMMEDIATE; ttype1=R;
tdp2=T_MID_CALL; tid2=T_SWITCH_HOOK_FLASH_IMMEDIATE
 ttype2=R; feature-server-id=FSPTC235; description=Three way call; grp-feature=N
```

**Step 2**
Add the service ID.
```
add service id=2;fname1=TWC;
```

**Step 3**
Assign the service to the subscriber.
```
add subscriber-service-profile sub-id=cisco-1;service-id=2;
```
Three-Way Calling Deluxe

The Three-Way Calling Deluxe (TWCD) feature allows a user to add a third party to an existing two party conversation without operator assistance. This includes adding a call received using call waiting deluxe.

Prerequisites

None.

Supported Interfaces

Not applicable

Provisioning TWCD

To provision TWCD, perform the following steps:

**Step 1**
Add the feature.

```
add feature fname=TWCD;tdp1=O_MID_CALL;tid1=O_SWITCH_HOOK_FLASH_IMMEDIATE;ttype1=R;
tdp2=T_MID_CALL;tid2=T_SWITCH_HOOK_FLASH_IMMEDIATE; ttype2=R;
feature-server-id=FSPTC325;- description=China Residential Three-way Calling Deluxe Feature;
```

**Step 2**
Add the service ID.

```
add service id=2;fname1=TWCD;
```

**Step 3**
Assign the service to the subscriber.

```
add subscriber-service-profile sub-id=china-1;service-id=2;
```

Provisioning TWCD for Centrex, and MLHG

To provision TWCD for Centrex, and MLHG perform Step 3 in the Provisioning TWCD section.
Time and Weather

The time and weather (TW) feature allows a subscriber to dial a number to get the time and weather information in his or her local area.

Prerequisites

None.

Supported Interfaces

Not applicable

Provisioning TW

To provision call types for TW, perform the following steps:

**Step 1** Create a TW dial plan.

```
add dial-plan id=dp1; digit-string=301-844; reqd-digits=10; dest-id=inter-rte-3333;
```

*Note* A dial plan profile must be added before you can add a dial-plan id.

**Step 2** Add a special call type for TW.

```
add special-call-type digit-string=844; call-type=TW; description=Time and Weather;
```

**Step 3** Verify that the digit string for TW was added.

```
show special-call-type digit-string=844;
```

Example Response:

Reply: Success: 1 entry found.

digit-string=844
CALL_TYPE=TW
DESCRIPTION=Time and Weather
Unified Messaging

The Unified Messaging (UM) feature allows voicemail calls to be routed to a Unified Messaging System. A subscriber can also activate the CF feature to a UM system.

Prerequisites

The Dial Plan table must be provisioned with a Voice Mail Calling dial plan.

Supported Interfaces

Table 6-13 shows the interface support between call origination and termination.

<table>
<thead>
<tr>
<th>Unified Messaging Supported Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>RGW termination</td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td>RGW origination</td>
</tr>
<tr>
<td>CAS origination</td>
</tr>
<tr>
<td>SS7 origination</td>
</tr>
<tr>
<td>ISDN origination</td>
</tr>
<tr>
<td>SIP origination</td>
</tr>
</tbody>
</table>

Provisioning Unified Messaging

This section shows how to provision a SIP trunk (identified with ID=99) in POP 1 on the Cisco BTS 10200 Softswitch towards the Unified Messaging (UM) server. In this example, the IP address and port of the UM server SIP interface is in the format of a fully qualified domain name called 'uone.lab.cisco.com:5060'. This trunk is added to the dial plan identified by “dp1.” The dial plan is associated to local subscribers on the Cisco BTS 10200 Softswitch who are forwarding their calls to the UM server, such as subscriber ID '24h1-4@cisco.cisco.com'. In this provisioning example, when the subscriber forwards calls to number 9722131234, the call is routed out the SIP trunk towards voice mail.

To provision unified messaging, perform the following steps:

**Step 1** Add the Softswitch trunk group profile.

```
add softsw-tg-profile id=99; protocol-type=sip;
```

**Step 2** Add the Softswitch trunk group for voicemail.

```
add trunk-grp id=99; softsw-tsap-addr=uone.lab.cisco.com:5060; call-agent-id=CA146;
tg-type=softsw; tg-profile-id=99; dial-plan-id=dp1; pop-id=1;
```
Usage-Sensitive Three-Way Calling

The Usage-Sensitive Three-Way Calling (USTWC) feature allows a subscriber to add a third party to an existing two-party conversation. It provides all of the functionality of TWC without specifically subscribing to the service.

Prerequisites

None.

Supported Interfaces

Not applicable

Provisioning USTWC

To provision USTWC, perform the following steps:

Step 1 Define USTWC in the Feature table.
add feature fname=USTWC; tp1=O_MID_CALL; t1=O_SWITCH_HOOK_FLASH_IMMEDIATE; ttype1=R; tdp2=T_MID_CALL; t2=T_SWITCH_HOOK_FLASH_IMMEDIATE; tt2=R; feature-server-id=FSPTC235; description=Usage Sensitive Three Way Calling Feature;

Step 2 Add the service ID.
add service id=999; fname=USTWC;
Step 3  Provision the Call Agent Configuration table.

add ca-config;type=default-office-service-id; datatype=integer; value=999;

Provisioning USTWC for Subscribers and Centrex

To provision USTWC for subscribers, perform the following steps:

Step 1  Change the subscriber’s Usage Sensitivity feature applicability flag.

change subscriber id=sub-1@abcd; USAGE-SENS=Y;

Step 2  Customize the feature denied flag for the subscriber as needed per individual requirements.

change subscriber-feature-data sub-id=subscriber-1; fname=USTWC; type1=DENIED value1=Y;

Warmline

The Warmline feature is a combination of a hotline and regular telephone line.

Prerequisites

The Warmline features requires subscriber subscription and a preset hotline number.

Supported Interfaces

Warmline originations are supported only on subscriber line interfaces.

Provisioning Warmline

To provision warmline, perform the following steps:

Step 1  Register the feature in the Office.

add feature fname=WARMLINE;tdp1=o-attempt-authorized; tid1=o-attempt-authd;
ttype1=R;feature-server-id=FSPTC335; description=Warmline; grp-feature=N;

Step 2  Provision the service in the Office.

add service id=special-srv; fname1=WARMLINE;

Step 3  Change the warmline dial-tone timeout parameter (if required).

add feature fname=WARMLINE; type1=TO; value1=6;
**Step 4**
Set the MGCP version of the MGW Profile of the media gateway that the subscriber line is associated with to non-0.1. This can be assigned to any of the fname tokens.

```
add mgw-profile id=plano-iad; mgcp-version=MGCP-1-0;
```

**Note**
MGCP 0.1 version does not support the TO signal completion report.

**Step 5**
Set the dial tone timeout as supported by the MGW. ASK PRAKASH

```
add mgw-profile id=plano-iad;
```

---

**Provisioning Warmline for Subscribers, Centrex, and MLHG**

To provision warmline for subscribers, Centrex, and MLHG, perform the following steps:

**Step 1**
Define the feature in the Feature table.

```
add feature fname=WARMLINE;tdpl=o-attempt-authorized;tid1=o-attempt-authd; ttype1=R; type1=TO; value1=6; feature-server-id=FSPTC235; description=warmline;
```

**Step 2**
Add the service to subscriber’s service profile.

```
add service id=556; fname=WARMLINE;
```

**Step 3**
Assign the service to the subscriber.

```
add subscriber-service-profile sub-id=24h1;service-id=556;
```

**Step 4**
Add the Warmline timeout target DN to the subscriber's feature data.

```
add subscriber-feature-data sub-id=24h1;fname=WARMLINE;type1=fdn1;active=y; value1=9722132401;
```
Provisioning Announcements

The Cisco BTS 10200 Softswitch has a set of announcements—prerecorded audio files—that are played to the caller when a call is released (does not go through). Service providers can control announcement features and create their own announcement files. The system default announcements, as well as any provider-created announcements, are stored on a gateway such as the Cisco AS5850. This chapter uses the Cisco AS5300 in its examples. Consult your specific gateway documentation for the procedures to set up announcements for your particular gateway.

Note

In order to work with Cisco BTS 10200 Softswitch, gateway audio files must be saved in 8-bit mu-Law encoded, Next/Sun Audio (AU) format (.au extension).

Caution

When creating custom announcement audio files, files must be saved in the .au format specified in the note above. This ensures that the system can access the file. Using any other format makes the file unreadable to the system.

This chapter consists of the following sections:

- Entering Gateway Information into the Cisco BTS 10200 Softswitch
- Entering an Announcement and Release Cause
- Creating Custom Announcements
- Cause Codes and Conditions
- Prerecorded Announcements

As with other trunks, announcement trunks are provisioned in a certain order. MGWs must be added before terminations and so forth. Use the flowchart given in Figure 7-1 to provision announcements.
Figure 7-1  Provisioning Announcements Flowchart

Provisioning Announcements Flowchart

ADD MGW PROFILE
  add mgw id=as5300; vendor=Cisco; description=Announcements;

ADD MGW
  add mgw id=c5300.131; tsap-addr=<AnnGW DNS/IP>; call-agent-id=CA101; mgw-profile-id=as5300; tgw=y; ans=y;

ADD ANNC-TG-PROFILE
  add annc-tg-profile id=annc-tgp;ivr=n;auto-answer=n; local-trunk-selection=n; description=annc trunk group profile;

ADD TRUNK-GRP
  add trunk-grp id=13; call-agent-id=CA101; tg_type=ANNC; tg-profile-id=annc-tgp;

ADD TERMINATION
  add termination prefix=S0/DS1-2/; port-start=1; port-end=24; type=trunk; mgcp-pkg-type=ANNC; mgw-id=c5300.131;

ADD TRUNK
  add trunk termination-prefix=S0/DS1-2/; termination-port-start=1; termination-port-end=24; cic-start=1; cic-end=24; tgn-id=13; mgw-id=c5300.131

ADD ROUTE
  add route id=annc-rt1; lcr=y; tgn1-id=13;

ADD ROUTE-GUIDE
  add route-guide id=annc1_rg; policy-type=ROUTE; policy-id=annc-rt1;

ADD ANNC-TRUNK
  add annc-trunk tgn-id=13; term-id=S0/D1-2[1...24]; mgw-id=c5300.131;

ADD ANNOUNCEMENT
  add announcement id=11; type=SYSTEM; route-guide-id=annc1_rg; announcement-file=ann_id_11.au;

ADD RELEASE-CAUSE
  add release-cause id=34; annc-id=11;

MGWs, trunks, and trunk terminations must be controlled in service after provisioning. Use the flowchart given in Figure 7-2 for the steps needed to control MGWs, trunks, and trunk terminations.
**Prerequisites**

Announcement circuits need to be provisioned. Each release cause value must be mapped to a particular announcement.

**Supported Interfaces**

Table 7-1 shows the interface support between call origination and termination for announcements.

<table>
<thead>
<tr>
<th>Announcement termination</th>
<th>origination</th>
</tr>
</thead>
<tbody>
<tr>
<td>RGW origination</td>
<td>X</td>
</tr>
<tr>
<td>CAS origination</td>
<td>X</td>
</tr>
<tr>
<td>SS7 origination</td>
<td>X</td>
</tr>
<tr>
<td>ISDN origination</td>
<td>X</td>
</tr>
<tr>
<td>SIP origination</td>
<td>X</td>
</tr>
</tbody>
</table>

**Entering Gateway Information into the Cisco BTS 10200 Softswitch**

This section describes how to enter information about a gateway into Cisco BTS 10200 Softswitch for announcements.
The steps in this chapter show examples of typical command-line interface (CLI) commands used to provision the announcement server data. For a complete list of command options and descriptions, see the *Cisco BTS 10200 Command Line Interface Reference Guide*.

If the media gateway (MGW), termination, trunk group, and routing have already been entered for the Cisco AS5300 on which this announcement is loaded, make sure the gateway is configured correctly using your specific gateway documentation.

These entities are entered in the Out Of Service (OOS) state. Use the control commands to place each entity In Service (INS) after all the data is entered.

**Step 1**

[Add the Cisco AS5300 MGW profile in the Cisco BTS 10200 Softswitch database.]

`add mgw-profile id=as5300;vendor=Cisco;packet-type=IP;lptime=10;hptime=20;mgcp-erqnt-unsupp=y;mgcp-hairpin-unsupp=y;mgcp-cmd-seq-unsupp=y;`

**Step 2**

Add the Cisco AS5300.

`add mgw id=vgw242; tsap-addr=190.101.10.50; call-agent-id=CA146; mgw-profile-id=as5300;tgw=y;`

**Step 3**

Add the announcement trunk group profile.

`add annc-tg-profile id=1; annc=y;ivr=n; annc-sig-type=TCL-CISCO; auto-answer=n;local-trunk-selection=y; add trunk-grp id=14; call=agent=CA146; tg-type=annc;cost=3;status=oos;tg-profile-id=1;`

**Step 4**

Add the Media Gateway Control Protocol (MGCP) announcement trunk group (TG).

`add trunk-grp id=14; call-agent-id=CA146; tg-type=annc; cost=3; status=oos; dchan-slot=0; dchan port=2; add annc-tg-profile id=1; annc=y;ivr=n; annc-sig-type=TCL-CISCO; auto-answer=n;local-trunk-selection=y; add trunk-grp id=14; call=agent=CA146; tg-type=annc;cost=3;status=oos;tg-profile-id=1;`

**Step 5**

Add the terminations for the Cisco AS5300.

`add termination prefix=S0/DS1-2/; port-start=1; port-end=24; mgw-id=vgw242; type=trunk;mgcp-pkg-type=annc; status=oos;`

**Step 6**

Add the trunk.

`add trunk termination-prefix=S0/DS1-2/; termination-port_start=1; termination-port_end=24; cic-start=1; cic-end=24; tgn-id=14; mgw-id=vgw242;`

**Step 7**

Add the routing information for the announcement TG.

`add route id=annnc3; tgn1-id=14;`

**Step 8**

Add the routing policy information.

`add route-guide id=annnc3; policy-type=route; policy-id=annnc3;`

**Step 9**

Add the announcement trunk group.

`add annnc-trunk tgn-id=14;term-id=S0/DS1-2/1;mgw-id=vgw242;`

**Step 10**

Add the announcement.

`add announcement id=11;type=system;route-guide-id=annnc3;announcement-file=ann_id_11.au;`
Chapter 7 Provisioning Announcements

Entering an Announcement and Release Cause

Use the procedure in this section to provision a system (standard) announcement in the Cisco BTS 10200 Softswitch. System announcement files are prerecorded and supplied with some Cisco gateways. Refer to the Cisco BTS 10200 System Description for a list of announcements. To create and provision a new (custom) announcement file, use the procedure in the “Creating Custom Announcements” section on page 7-5 instead.

Step 1 Add the announcement.
```
add announcement id=19; type=system; announcement-file=ann_id_19.au; num-repeat=2;
route-guide=annc3; description=this party has moved to a new extension number;
```

Note Do not use hyphens in announcement filenames. Use only underscores.

Step 2 Associate this announcement file with a specific release cause ID number.
```
change rel-cause id=22; annc-id=19; description=number changed;
```

Creating Custom Announcements

This section describes the following:
- Creating the Announcement and Downloading to the Cisco AS5300, page 7-5
- Entering Announcement Data for a Custom Announcement, page 7-6

Creating the Announcement and Downloading to the Cisco AS5300

This section describes how to create an announcement and download it to the gateway.

Step 1 Record the new announcement and save the file in 8-bit mu-Law encoded, Next/Sun AU format (.au extension). Do not use hyphens in announcement filenames. Use only underscores. The custom file must be named in the following format:
```
<ann_id_1xxxx.au > (xxxx = 1 to 1000)
```
Step 2  Download the new file to the flash memory of the Cisco AS5300. Use the procedures in the Cisco AS5300 user documentation.

Entering Announcement Data for a Custom Announcement

This section describes how to enter custom announcement data.

Step 1  Enter the announcement data. The ID for a custom announcement must be a number between 501 and 1000. Leading zeros in the announcement ID number are not permitted. Do not use hyphens in announcement filenames. Use only underscores.

    add announcement id=777; type=custom; announcement-file=message-777.au; num-repeat=2; route-guide=annnc3; description=this party has moved to a new extension number;

Step 2  Associate the new announcement file with a specific release cause ID number:

    change release-cause id=22; annnc-id=777; description=number changed;

Cause Codes and Conditions

The Cisco BTS 10200 Softswitch supports announcement features by sending defined cause codes to the service provider’s announcement server. These cause codes, and conditions encountered, are listed in Table 7-2.

<table>
<thead>
<tr>
<th>Cause Code Number for Condition Encountered</th>
<th>Cause Code for Condition Encountered</th>
<th>Condition Encountered</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>No circuit available</td>
<td>All trunks busy</td>
</tr>
<tr>
<td>Switching Blockages</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Call rejected</td>
<td>Temporary network failure condition or internal office failure</td>
</tr>
<tr>
<td>28</td>
<td>Address incomplete</td>
<td>Partial digits received</td>
</tr>
<tr>
<td>29</td>
<td>Facility rejected</td>
<td>Temporary network failure condition or internal office failure</td>
</tr>
<tr>
<td>Misdialing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>157</td>
<td>Prefix 1 or 0 present</td>
<td>Prefix access code dialed in error</td>
</tr>
<tr>
<td>156</td>
<td>Prefix 1 or 0 absent</td>
<td>Prefix not dialed, prefix 1 not dialed, or prefix 0 not dialed</td>
</tr>
<tr>
<td>159</td>
<td>HNPA area code absent</td>
<td>10-digit HNPA dialing area code not dialed</td>
</tr>
<tr>
<td>Numbers Intercepted</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 7-2 Announcement Cause Codes and Conditions Encountered (continued)

<table>
<thead>
<tr>
<th>Cause Code Number for Condition Encountered</th>
<th>Cause Code for Condition Encountered</th>
<th>Condition Encountered</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>No route to destination</td>
<td>No route to destination, invalid number of digits or invalid prefix</td>
</tr>
<tr>
<td>28</td>
<td>Address incomplete</td>
<td>No route to destination, invalid number of digits or invalid prefix</td>
</tr>
<tr>
<td>1</td>
<td>Unallocated number</td>
<td>Unallocated NPA code, vacant code or changed number</td>
</tr>
<tr>
<td>22</td>
<td>Number changed</td>
<td>Vacant or disconnected number</td>
</tr>
<tr>
<td>1</td>
<td>Unallocated number</td>
<td>Vacant or disconnected number</td>
</tr>
<tr>
<td>22</td>
<td>Number changed</td>
<td>Vacant or disconnected number</td>
</tr>
<tr>
<td>27</td>
<td>Destination out of order</td>
<td>Temporarily disconnected number</td>
</tr>
<tr>
<td>151</td>
<td>Temporarily disconnected</td>
<td>Temporarily disconnected number</td>
</tr>
</tbody>
</table>

**COS Restrictions**

<table>
<thead>
<tr>
<th>Cause Code</th>
<th>Condition Encountered</th>
</tr>
</thead>
<tbody>
<tr>
<td>163</td>
<td>Feature not subscribed</td>
</tr>
<tr>
<td>164</td>
<td>Auth Code invalid</td>
</tr>
<tr>
<td></td>
<td>Unassigned custom calling feature</td>
</tr>
</tbody>
</table>

**InterLATA Call Handling**

<table>
<thead>
<tr>
<th>Cause Code</th>
<th>Condition Encountered</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>No route to specified transit network</td>
</tr>
<tr>
<td></td>
<td>No route to IXC</td>
</tr>
</tbody>
</table>

**LNP**

<table>
<thead>
<tr>
<th>Cause Code</th>
<th>Condition Encountered</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>Misrouted call to ported number</td>
</tr>
<tr>
<td>42</td>
<td>Switching equipment congestion</td>
</tr>
<tr>
<td></td>
<td>Switching equipment congestion on route to new number</td>
</tr>
</tbody>
</table>

**Caller ID Delivery Blocking**

<table>
<thead>
<tr>
<th>Cause Code</th>
<th>Condition Encountered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1053</td>
<td>Anonymous call reject</td>
</tr>
<tr>
<td></td>
<td>The called party is not accepting calls that have caller ID blocked</td>
</tr>
</tbody>
</table>

## Prerecorded Announcements

The Cisco BTS 10200 Softswitch has a set of prerecorded audio files that can be played to the caller when a call does not go through. The service provider can provision any of these recordings to play when a particular cause code is activated in the system. A list of these announcements are provided in Table 7-3. The mappings can be changed using the change release cause CLI command. Service providers can also enter new announcement file names and use their own announcement files. However, the announcement files must be in 8-bit mu-Law encoded, Next/Sun AU, format (.au extension).
### Table 7-3 Cisco BTS 10200 Prerecorded Announcements

<table>
<thead>
<tr>
<th>Announcement File Name ann_id_xx.au</th>
<th>Announcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>If you’d like to make a call, please hang up and try again. If you need help, hang up and then dial your operator.</td>
</tr>
<tr>
<td>11</td>
<td>We’re sorry, all circuits are busy now. Please try your call again later.</td>
</tr>
<tr>
<td>12</td>
<td>We’re sorry, your call did not go through. Please try your call later.</td>
</tr>
<tr>
<td>14</td>
<td>We’re sorry, it is not necessary to dial a 1 or 0 when calling this number. Please hang up and try your call again.</td>
</tr>
<tr>
<td>15</td>
<td>We’re sorry, you must first dial a 1 or 0 when calling this number. Please hang up and try your call again.</td>
</tr>
<tr>
<td>16</td>
<td>We’re sorry. When placing a local call it is now necessary to dial an area code followed by the 7-digit local number. Please hang up and redial using the complete 10-digit number.</td>
</tr>
<tr>
<td>17</td>
<td>We’re sorry, your call cannot be completed as dialed. Please check the number and dial again.</td>
</tr>
<tr>
<td>18</td>
<td>The number you dialed is not in service. Please check the number and dial again.</td>
</tr>
<tr>
<td>19</td>
<td>We’re sorry, you have reached a number that has been disconnected or no longer in service. If you feel you have reached this recording in error, please check the number and try your call again.</td>
</tr>
<tr>
<td>20</td>
<td>The party you are calling has temporarily disconnected their service.</td>
</tr>
<tr>
<td>21</td>
<td>We’re sorry, your call cannot be completed as dialed from the phone you are using. Please read the instruction card and dial again.</td>
</tr>
<tr>
<td>23</td>
<td>We’re sorry, it is not necessary to dial a long-distance company access code for the number you have dialed. Please hang up and try your call again.</td>
</tr>
<tr>
<td>24</td>
<td>We’re sorry, your call cannot be completed as dialed. Please check your instruction manual or call the business office for assistance.</td>
</tr>
<tr>
<td>50</td>
<td>We’re sorry, your call cannot be completed with the access code you dialed. Please check the code and try again, or call your long-distance company for assistance.</td>
</tr>
<tr>
<td>51</td>
<td>We’re sorry, the long-distance company you have dialed is experiencing a temporary service problem. Please try your call again later.</td>
</tr>
<tr>
<td>52</td>
<td>We’re sorry, a long-distance company access code is required for the number you have dialed. Please dial your call again with the access code.</td>
</tr>
<tr>
<td>53</td>
<td>We’re sorry, your call cannot be completed with the access code you dialed. Please check the code and try again, or call your long-distance company for assistance.</td>
</tr>
<tr>
<td>54</td>
<td>We’re sorry, your call cannot be completed with the access code you dialed. Please check the code and try again, or call your long-distance company for assistance.</td>
</tr>
<tr>
<td>55</td>
<td>We’re sorry, it is not necessary to dial a long-distance company access code for the number you have dialed. Please hang up and try your call again.</td>
</tr>
</tbody>
</table>
### Table 7-3  Cisco BTS 10200 Prerecorded Announcements (continued)

<table>
<thead>
<tr>
<th>Announcement File Name</th>
<th>Announcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>56</td>
<td>We’re sorry, the long-distance company you have selected is unable to complete your call at this time. Please contact your long-distance company for assistance.</td>
</tr>
<tr>
<td>57</td>
<td>We’re sorry, the long-distance company you have selected is unable to complete your call at this time. Please contact your long-distance company for assistance.</td>
</tr>
<tr>
<td>61</td>
<td>Your call has been properly delivered, but the party you are trying to reach is not accepting calls from callers who do not allow delivery of their telephone number. Please hang up, do not block the delivery of your number, and call again.</td>
</tr>
</tbody>
</table>
Provisioning SS7

This chapter describes the steps necessary to provision Signaling System 7 (SS7) on the Cisco BTS 10200 Softswitch.

This chapter contains the following sections:

- Building the SS7 Network Configuration, page 8-1
- Provisioning the Cisco BTS 10200 Softswitch, page 8-25
- SS7 Trunk Group Status and Control, page 8-27

Building the SS7 Network Configuration

This section describes how to set up SS7 links between the Cisco BTS 10200 Softswitch and a signal transfer point (STP) in the public switched telephone network (PSTN) network. Once you are logged in to the Cisco BTS 10200 Softswitch system, perform the remainder of the procedure using the Signalware graphical user interface (GUI).

Table 8-1 provides an overview of setting up SS7 links.

<table>
<thead>
<tr>
<th></th>
<th>Overview of Setting Up SS7 Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log on to the Call Agent.</td>
</tr>
<tr>
<td>2.</td>
<td>Create a local point code.</td>
</tr>
<tr>
<td>3.</td>
<td>Create a linkset.</td>
</tr>
<tr>
<td>4.</td>
<td>Create a signaling link.</td>
</tr>
<tr>
<td>5.</td>
<td>Create a combined linkset.</td>
</tr>
<tr>
<td>6.</td>
<td>Create a route set.</td>
</tr>
<tr>
<td>7.</td>
<td>Create an outbound global title translation.</td>
</tr>
<tr>
<td>8.</td>
<td>Optional. Alternate provisioning for automatic callback (AC) and automatic recall (AR) services.</td>
</tr>
</tbody>
</table>
Logging On to the Call Agent (Windows Environment)

This section applies only to Windows users.

This section describes how to log on to the Cisco BTS 10200 Softswitch Call Agent in a Windows environment.

The Omni application can run on Windows 98, Windows NT 4.0, and later platforms, running Exceed 6.2 or later. Run Exceed from the Start menu before initiating a Secure Shell (SSH) session to the Call Agent (CA).

There are two Call Agents in the system:
- Side A (primary)
- Side B (secondary)

You can perform this procedure on either Call Agent.

Note
In all the steps in this procedure, enter the commands as shown; some commands are case-sensitive. Press the Enter key at the end of each command.

Step 1
From the Windows desktop, choose Start > Run.
A Run dialog box opens.

Step 2
Enter cmd.

Step 3
At the login prompt, enter root.

Step 4
At the password prompt, enter root.

Step 5
At the prompt, enter c: or the letter for your local hard drive.

Step 6
SSH to your Call Agent.

Step 7
At the login prompt, enter your login ID.

Step 8
At the password prompt, enter your password.

Step 9
Navigate to the tools directory using the following command:
`cd /opt/omni/tools`

Step 10
List files using the following command and look for the jre-1_2_2_2_006-win-i.exe file:
`ls`

Step 11
Enter bin.

Step 12
Get the jre-1_2_2_2_006-win-i.exe file.
`get jre-1_2_2_2_006-win-i.exe`

Look for a message that says your file has been successfully transferred.

Step 13
Close the command prompt window.

Step 14
Go to the local drive where you transferred the file.

Step 15
Double-click the filename to execute the Javasoft 1.2 file.

Step 16
Select the defaults.
Step 17  Repeat Step 9 through Step 16 for the Signalware.jar file. The directory in Step 9 will be replaced with /opt/omni/classes.

Note  To find out the IP address of your workstation, choose Start > Run and enter cmd. Click OK. This opens a cmd.exe window. At the prompt, enter ipconfig and press Return.

Launching the JavaSoft Program

To launch the JavaSoft program so you can run the Signalware GUI, perform the following steps:

Step 1  From the Windows desktop, choose Start > Run.
       A Run dialog box opens.

Step 2  Enter cmd.

Step 3  At the C:\ prompt, enter the following:
       Progra~1\JavaSoft\JRE\1.2\bin\java.exe -classpath C:\Signalware.jar ulticom.gui.Signalware.

       The Ulticom window opens, then the Signalware login window.

Step 4  At the login prompt, enter omni.

Step 5  At the password prompt, enter omni.

Step 6  Enter the following information at each prompt:
       SHM: 225
       Computing Element: <your call agent>
       Port: accept the default

Step 7  To bring up the main menu, click login.

Note  You must keep the command prompt window open to run the Signalware GUI. The Signalware GUI screens in this chapter show screens with sample data added. Enter the data for your own system as specified by your network administrator or local work order.
Creating a Local Point Code

To create a local point code, perform the following steps:

**Step 1**
Open the Signalware GUI application by entering the following command:

```
[OmniMenu]
```

The Signalware User Interface window appears. Status and control reporting is available via this menu.

**Step 2**
To provision the local Call Agent point code, choose `a7n1 > Own Point Code`.

The Open Point Code window opens.
Step 3  To create a point code, choose **Action > Create**.

![Create Own Point Code window](image)

The Create Own Point Code window opens.

Step 4  Enter the local point code and the network indicator data, then click **OK** or **Apply**.

![Create Own Point Code](image)
Creating a Linkset

To create a linkset, perform the following steps:

**Step 1** From the Signalware User Interface window, choose **a7n1 > Link Sets.**

The Link Sets window opens.
**Step 2** To create a link set, choose *Action > Create*. 

The Create Link Set window opens.
Step 3 Enter the linkset name, adjacent point code, and linkset type (A for access links to a signal transfer point (STP)) and then click OK or Apply.

Creating a Signaling Link

To create a signaling link, perform the following steps:

Step 1 From the Signalware User Interface window, choose a7n1 > Signaling Links.
The Signaling Links window opens.

**Step 2**

To create a new link, choose **Action > Create**.

The Create Signaling Link window opens.
Step 3  Enter the applicable parameters and click **OK** or **Apply**.

![Create Signaling Link](image)

**Note**  
*Channel* refers to the timeslot on the T1 channel.

**Note**  
The value for signaling link code (SLC) on the Call Agent must be the same as the SLC on the STP.

**Note**  
The port parameter maps the link to a specific Omni board. Refer to the /opt/omni/conf/portConf.225 file for mapping of port number to boards. A typical system has two Omni boards on each Call Agent box with the following port mappings:  
- First board on primary side—ports 0-15  
- Second board on primary side—ports 16-31  
- First board on secondary side—ports 32-47  
- Second board on secondary side—ports 48-63
Creating a Combined Linkset

To create a combined linkset, perform the following steps:

**Step 1**  From the Signalware User Interface window, choose **a7n1 > Combined Linksets**.

![Combined Link Sets window](image)

The Combined Link Sets window opens.
Step 2  To create a combined link, choose **Action > Create**.

The Create Combined Link Set window opens.

Step 3  Enter the combined link set and link set name data. Click **OK** or **Apply**.
Creating a Route Set

To create a route set, perform the following steps:

**Step 1**  From the Signalware User Interface window, choose a7n1 > Route Sets.

The Route Sets window opens.
Step 2  To create a new Route Set, choose **Action > Routesets**.

The Create Route Set window opens.
Step 3  To create a new Route Set, enter the required parameters, then click OK or Apply.
Step 4  
To create routes to destination point codes beyond the STP pair, use the Combined Linkset to the STPs.

Creating a Global Title Translation

Cisco BTS 10200 Softswitch 8xx and local number portability (LNP) features require global title translation (GTT) on the SS7 network. Default values for GTT type and subsystem number (SSN) are defined at software installation time. Table 8-2 shows the typical default values.

---

The GTT and SSN values for your system are available from your SS7 service provider.

---

Table 8-2  Subsystem Number and Translation Type Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example of Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssnl02</td>
<td>Subsystem number for toll-free (800) service</td>
<td>254</td>
</tr>
<tr>
<td></td>
<td>(248 is typically used for AIN 0.1, and 254 for TCAP)</td>
<td></td>
</tr>
<tr>
<td>ssnlnp</td>
<td>Subsystem number for LNP service</td>
<td>247</td>
</tr>
<tr>
<td>ssncnam</td>
<td>Subsystem number for calling name delivery (CNAM) service</td>
<td>232</td>
</tr>
</tbody>
</table>
To create GTT for your Cisco BTS 10200 Softswitch, perform the following steps:

**Step 1**  
From the Signalware User Interface window, choose **a7n1 > Global Title > Outbound.**

The Outbound Global Title window opens.
Step 2  To create the GTT values, choose **Action > Create**.

The Create Outbound Global Title window opens.
Step 3 Enter the GTT data for your system, then click OK or Apply.

![Create Outbound Global Title](image)

Step 4 Click Cancel to close the a7n1-Create Global Title window.

Step 5 To log off the Call Agent, enter exit at the host prompt in the XTerm window.

---

Alternate Provisioning for Automatic Callback and Automatic Recall Services

This section describes an alternative Omni provisioning method that uses network and/or cluster routes. This method eliminates the need to configure remote subsystem numbers (SSNs) for each end office to facilitate responses to inbound TCAP queries for the AC, AR services.

Caution This alternate provisioning method requires a full outage on the Call Agent, FSPTC, and FSAIN when done on an existing Cisco BTS 10200 Softswitch installation.

Perform the following steps to provision AC and AR services using network and/or cluster routes:

Step 1 Create a file contains the following line:

```
SC_REMSSN_CK=NO
```

Step 2 Save this file under the filename:

```
scmg_conf_info
```

Step 3 Put this configuration file in the following directory for both primary and secondary Call Agents:

```
/opt/omni/conf
```
Chapter 8  Provisioning SS7

Building the SS7 Network Configuration

Step 4  Configure the necessary cluster and/or network route sets. Omni allows a wildcard on clusters and members. “X” is the wildcard indication. For example:

- a cluster route looks like this: 220-10-X
- a network route looks like this: 220-X-X

Perform the following commands at the Omni provisioning prompt. For example, if the NPA-digit 512 resides in the remote switch with point-code 1-3-1 and the NPA-digit 612 is in the local switch with point-code 1-2-1, the provisioning is:

CREATE-GT:TT=251,NP=ISDN-TEL,DIG="512",PC=1-3-1,SSN=251,RI=DEF;
CREATE-GT:TT=251,NP=ISDN-TEL,DIG="612",PC=1-2-1,SSN=251,RI=DEF;

Termhandler

The Omni Termhandler interface is an alternative to using the Omni GUI. Man pages are available for all of the Termhandler commands in the /opt/omni/man/cat8 directory on the Call Agent. To get help on usage or syntax for any command, enter man <command-name> (for example, man create-slk.)

The following is a sample Termhandler script:

Script started on Thu Jan 17 15:26:01 2002
prica18#
prica18# termhandler -node a7n1 <<<<<<<<<<< start termhandler

+-------------+    Terminal Handler [Started]
| TermHandler |    Copyright 1993, 1994 DGM&S
+-------------+    All Rights Reserved

Usage: Filename: - to execute from a file
MML command: - series of mml command(s)

OMNI [17 Jan 2002 15:26:13] #1:display-ospc; <<<<<<<<<<< display own point code

Send [DISPLAY-OSPC;]? [Y/N]y
Sent MML command #1 to ACTV_PM, cmd[DISPLAY-OSPC;]
starting 5 min. timer...
1  [17 Jan 2002 15:26:22]
DISPLAY-OSPC;

--- OWN SIGNALLING POINT CODE ---

OWN PC Network Indicator
3-018-100 NAT0 Primary

Usage: Filename: - to execute from a file
MML command: - series of mml command(s)

OMNI [17 Jan 2002 15:26:22] #2:display-slk;

Send [DISPLAY-SLK;]? [Y/N]y
Sent MML command #2 to ACTV_PM, cmd[DISPLAY-SLK;] <<<<<<<<<<< display signalling links
starting 5 min. timer...
2  [17 Jan 2002 15:26:31]
### DISPLAY-SLK;

--- SIGNALLING LINKS ---

<table>
<thead>
<tr>
<th>Name</th>
<th>Nbr</th>
<th>LSet Name</th>
<th>LSet Nbr</th>
<th>SLC Port</th>
<th>Chan</th>
<th>Speed</th>
<th>ADPC</th>
<th>State</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>LNK0</td>
<td>1</td>
<td>LSET0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>56000</td>
<td>3-018-000</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>LNK1</td>
<td>2</td>
<td>LSET0</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>56000</td>
<td>3-018-000</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

--- SIGNALLING LINK STATUS LEGEND ---

- i - installed
- n - link normal
- b - not locally blocked
- o - not remotely blocked
- l - not locally inhibited
- r - not remotely inhibited
- a - SLT Alignment enabled
- p - SLT Periodic enabled

Usage: Filename: - to execute from a file
MML command: - series of mml command(s)

OMNI [17 Jan 2002 15:26:31] #3:deact-slk:slk=lnk0; <<<<<<<< deactivate link 0

Send [DEACT-SLK:SLK=LNK0;]? [Y/N]y
Sent MML command #3 to ACTV_PM, cmd[DEACT-SLK:SLK=LNK0;]
starting 5 min. timer...
3    [17 Jan 2002 15:27:17]
DEACT-SLK:SLK=LNK0;
M COMPLETED

OMNI [17 Jan 2002 15:27:17] #4:actv-slk:slk=lnk0;  <<<<<<<< activate link 0

Send [ACTV-SLK:SLK=LNK0;]? [Y/N]y
Sent MML command #4 to ACTV_PM, cmd[ACTV-SLK:SLK=LNK0;]
starting 5 min. timer...
ACTV-SLK:SLK=LNK0;
M COMPLETED

OMNI [17 Jan 2002 15:27:28] #5:display-designation; <<<<<<display designated processes

Send [DISPLAY-DESIGNATION;]? [Y/N]y
Sent MML command #5 to ACTV_PM, cmd[DISPLAY-DESIGNATION;]
starting 5 min. timer...
5    [17 Jan 2002 15:27:35]
DISPLAY-DESIGNATION;
Designatable Process copies for system 225
Building the SS7 Network Configuration

<table>
<thead>
<tr>
<th>Process</th>
<th>Active Copy</th>
<th>Standby Copy</th>
<th>Idle Copies</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAP</td>
<td>prica18</td>
<td>secca18</td>
<td></td>
</tr>
<tr>
<td>PM</td>
<td>prica18</td>
<td>secca18</td>
<td></td>
</tr>
<tr>
<td>PortMon</td>
<td>prica18</td>
<td>secca18</td>
<td></td>
</tr>
<tr>
<td>OOSVR</td>
<td>prica18</td>
<td>secca18</td>
<td></td>
</tr>
<tr>
<td>GUISVR</td>
<td>prica18</td>
<td>secca18</td>
<td></td>
</tr>
<tr>
<td>a7n1_NM</td>
<td>prica18</td>
<td>secca18</td>
<td></td>
</tr>
<tr>
<td>a7n1_MEAS</td>
<td>prica18</td>
<td>secca18</td>
<td></td>
</tr>
<tr>
<td>a7n1_L3MTP</td>
<td>prica18</td>
<td>secca18</td>
<td></td>
</tr>
<tr>
<td>a7n1_SCMG</td>
<td>prica18</td>
<td>secca18</td>
<td></td>
</tr>
<tr>
<td>a7n1_ISMG</td>
<td>prica18</td>
<td>secca18</td>
<td></td>
</tr>
<tr>
<td>a7n1_TCMG</td>
<td>prica18</td>
<td>secca18</td>
<td></td>
</tr>
<tr>
<td>a7n1_ctrl</td>
<td>prica18</td>
<td>secca18</td>
<td></td>
</tr>
</tbody>
</table>

Usage: Filename: - to execute from a file
MML command: - series of mml command(s)

OMNI [17 Jan 2002 15:27:35] #6:display-rset; <<<<<<<<<<< display route sets

Send [DISPLAY-RSET;]? [Y/N]y
Sent MML command #6 to ACTV_PM, cmd[DISPLAY-RSET;]
starting 5 min. timer...
6 [17 Jan 2002 15:27:55]
DISPLAY-RSET;

--- ROUTE SET ---
Name    DPC        State   Status  Routing Method
RSET0   3-018-000  ACTIVE  ac0     STP

--- ROUTES ---
Name    CLS Name    Status
LSET0   CLSET0      ax
LSET1   CLSET0      Ax

--- ROUTE SET ---
Name    DPC        State   Status  Routing Method
RSET1   3-018-001  ACTIVE  ac0     STP

--- ROUTES ---
Name    CLS Name    Status
LSET1   CLSET0      Ax
LSET0   CLSET0      ax

--- ROUTE SET ---
Name    DPC        State   Status  Routing Method
RSET2   3-018-101  ACTIVE  ac0     Member
More? [Yes/No] n

Usage: Filename:    - to execute from a file
MML command: - series of mml command(s)

OMNI [17 Jan 2002 15:28:01] #7:display-rset:rset=rset2;  <<<< display route set 2

Send [DISPLAY-RSET:RSET=RSET2;]? [Y/N]y
Sent MML command #7 to ACTV_PM, cmd[DISPLAY-RSET:RSET=RSET2;]
starting 5 min. timer...
7 [17 Jan 2002 15:28:19]
DISPLAY-RSET:RSET=RSET2;

--- ROUTE SET ---
Name       DPC        State   Status  Routing Method
RSET2     3-018-101     ACTIVE     ac0  Member

--- ROUTES ---
Name        CLS Name        Status
LSET0       CLSET0           ax
LSET1       CLSET0           Ax

--- ROUTE SET STATUS LEGEND ---
a - PC accessible               A - PC inaccessible
c0 - route set not congested    Cx - route set congested to level x

--- ROUTE STATUS LEGEND ---
a - link set available          A - link set not available
x - transfer allowed            X - transfer prohibited

Usage: Filename:    - to execute from a file
MML command: - series of mml command(s)

OMNI [17 Jan 2002 15:28:19] #8:inh-rset;rset=rset2;  <<<<<< command line error (;
instead of :)

Send [INH-RSET;]? [Y/N]y
Sent MML command #8 to ACTV_PM, cmd[INH-RSET;]
starting 5 min. timer...
8 [17 Jan 2002 15:28:45]
INH-RSET;

Send [RSET=RSET2;]? [Y/N]y
Sent MML command #8 to ACTV_PM, cmd[RSET=RSET2;]
starting 5 min. timer...
8 [17 Jan 2002 15:28:51]
RSET=RSET2;
M DENY
IISP
Syntax error at or after: RSET

Usage: Filename:    - to execute from a file
MML command: - series of mml command(s)

Send [INH-RSET:RSET=RSET2;]? [Y/N]y
Sent MML command #9 to ACTV_PM, cmd[INH-RSET:RSET=RSET2;]
starting 5 min. timer...
9    [17 Jan 2002 15:29:12]
INH-RSET:RSET=RSET2;
M COMPLETED

Usage: Filename: - to execute from a file
MML command: - series of mm command(s)


Send [ALW-RSET:RSET=RSET2;]? [Y/N]y
Sent MML command #10 to ACTV_PM, cmd[ALW-RSET:RSET=RSET2;]
starting 5 min. timer...
10   [17 Jan 2002 15:29:22]
ALW-RSET:RSET=RSET2;
M COMPLETED

Usage: Filename: - to execute from a file
MML command: - series of mm command(s)

OMNI [17 Jan 2002 15:29:22] #11:q      <<< quit from termhandler
prica18#
prica18#
prica18# cd /opt/omni/man/cat8
prica18#
prica18# ls create*
create-asp.8  create-gt.8  create-ospc.8  create-rset.8
create-assoc.8 create-lset.8  create-process.8  create-slk.8
create-cc-client.8 create-m3ba-prf.8 create-remote-host.8
create-tcap-client.8
create-clset.8  create-m3ba.8  create-remssn.8  create-xconn.8
create-cpc.8    create-mm1-client.8 create-repcc.8
create-event-client.8 create-na.8  create-rk.8
prica18#
prica18#
prica18# ls display*
display-active-client.8  display-gt.8  display-purge.8
display-assoc.8  display-gtp.8  display-remote-host.8
display-bkup.8  display-lk-license.8  display-remssn.8
display-cc-client.8  display-m3ba.8  display-rk.8
display-clset.8  display-m3ba-prf.8  display-rset.8
display-client.8  display-m3ba-trace.8  display-slk.8
display-cpc.8  display-m3ua-timer.8  display-ss7-node.8
display-designation.8  display-mml-category.8  display-tcap-client.8
display-efilter.8  display-ml1-client.8  display-timer.8
display-event-category.8  display-na.8  display-xconn.8
display-event-client.8  display-ospc.8
prica18#
prica18#
prica18# ls delete*
delete-asp.8  delete-lset.8  delete-remote-host.8
delete-assoc.8  delete-m3ba-prf.8  delete-remssn.8
delete-cc-client.8 delete-m3ba.8  delete-repcc.8
delete-clset.8  delete-mm1-category.8  delete-rk.8
delete-cpc.8  delete-mm1-client.8  delete-rset.8
delete-event-category.8  delete-na.8  delete-slk.8
delete-event-client.8  delete-ospc.8  delete-tcap-client.8
Here’s an example of the termhandler commands used to provision a simple network configuration with A links to an STP and routes to SPs beyond the STPs.

CRTE-OSPC:PC=3-18-100,NI=NAT0;
CRTE-LSET:LSET=LSET0,PC=3-18-0,TYPE=A;
CRTE-SLK:SLK=LNK0,LSET=LSET0,SLC=0,SPEED=56K,PORT=0,CHANNEL=1;
CRTE-SLK:SLK=LNK1,LSET=LSET0,SLC=1,SPEED=56K,PORT=4,CHANNEL=1;
CRTE-LSET:LSET=LSET1,PC=3-18-1,TYPE=A;
CRTE-CLSET:CLSET=CLSET0,LSET=LSET0&LSET1;
CRTE-RSET:RSET=RSET0,PC=3-18-0,RTES=CLSET0;
ALW-RSET:RSET=RSET0;
CRTE-RSET:RSET=RSET1,PC=3-18-1,RTES=CLSET0;
ALW-RSET:RSET=RSET1;
CRTE-RSET:RSET=RSET2,PC=3-18-101,RTES=CLSET0;
ALW-RSET:RSET=RSET2;
CRTE-RSET:RSET=RSET3,PC=3-18-102,RTES=CLSET0;
ALW-RSET:RSET=RSET3;
CRTE-RSET:RSET=RSET4,PC=3-18-103,RTES=CLSET0;
ALW-RSET:RSET=RSET4;
ACTV-SLK:SLK=LNK0;
CHG-SLK:SLK=LNK0,PER=Y;
ACTV-SLK:SLK=LNK1;
CHG-SLK:SLK=LNK1,PER=Y;
CREATE-GT:TT=11,NP=ISDN-TEL,DIG="5",PC=3-18-0,SSN=247,RI=DEF;
CREATE-GT:TT=254,NP=ISDN-TEL,DIG="800",PC=3-18-0,SSN=254,RI=DEF;

### Table 8-3  Overview of SS7 Trunk Group Provisioning

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Add a media gateway profile (mgw-profile).</td>
</tr>
<tr>
<td>2.</td>
<td>Add the media gateway (mgw).</td>
</tr>
<tr>
<td>3.</td>
<td>Add SS7 terminations.</td>
</tr>
<tr>
<td>4.</td>
<td>Add an SS7 trunk group profile.</td>
</tr>
<tr>
<td>5.</td>
<td>Add the SS7 trunk group (TG).</td>
</tr>
<tr>
<td>6.</td>
<td>Add the SS7 trunk.</td>
</tr>
<tr>
<td>7.</td>
<td>Control the SS7 trunk group into service.</td>
</tr>
</tbody>
</table>
The following example commands are typical, and must be adapted to your specific system. For a detailed description of each command and all the tokens, see the Cisco BTS 10200 Command Line Interface Reference Guide.

If an “Unknown” state is returned when provisioning SS7 trunks, it means that the hardware is present but not provisioned with any data—the hardware is not being used by the system.

Step 1
If not already done on your system, add a media gateway profile.

```
add mgw-profile id=3660; vendor=cisco
```

Step 2
Add the media gateway.

```
add mgw id=tgw2; tsap-addr=190.101.10.221; call-agent-id=CA101; mgw-profile-id=as5300; tgw=y;
```

Step 3
Add an SS7 termination.

```
add termination prefix=s0/ds1-0/; port-start=1; port-end=24; mgw-id=tgw2; type=trunk;
```

Tip
The SS7 termination ID is generated by concatenating prefix and port-start value and termination port numbers. The termination port number starts with port-start and is incremented until the port number value reaches port-end.

See Figure 8-1 for an example of termination ID values for the Cisco AS5300 Voice Gateway.

Figure 8-1  Example of SS7 Terminations

Step 4
If not already done on your system, add an SS7 trunk group profile.

```
add trunk-group-profile id=101; type=ss7;
```

Note
Your local work order should indicate whether you need a new SS7 trunk group profile.
Chapter 8  Provisioning SS7

SS7 Trunk Group Status and Control

This section describes how to check the status of an SS7 trunk group and control an SS7 trunk in-service (INS) and out-of-service (OOS).

To check trunk group status and control, perform the following steps.

Note
In Release 3.5, when performing multiple control commands in immediate succession, always wait at least 1 second before performing the second command. For example:
control trunk-grp tgn-id=129; mode=forced; target-state=oos; (wait 1 second)
control trunk-grp tgn-id=129; mode=forced; target-state=ins;

Step 1 Enter the following command to check the status of an SS7 trunk group:

status trunk-grp id=ss7_tg2;

Reply Example:
RESULT -> ADM configure result in success
REASON -> ADM executed successful
ADMIN STATE -> ADMIN_INS
OPER STATE -> Trunk group in-service
TGN ID -> ss7_tg2

Step 2  Enter the following command to control an SS7 trunk group OOS:

```
control trunk-grp id=ss7_tg2; mode=forced; target-state=OOS;
```

Reply Example:
Reply : Success: CLI change successful
INITIAL STATE -> ADMIN_INS
REQUEST STATE -> ADMIN_OOS
RESULT STATE -> ADMIN_OOS
FAIL REASON -> ADM found no failure
REASON -> ADM executed successful
RESULT -> ADM configure result in success
TGN ID -> ss7_tg2

Step 3  Enter the following command to control an SS7 trunk group INS:

```
control trunk-grp id=ss7_tg2; mode=forced; target-state=INS;
```

Reply Example:
Reply : Success: CLI change successful
INITIAL STATE -> ADMIN_OOS
REQUEST STATE -> ADMIN_INS
RESULT STATE -> ADMIN_INS
FAIL REASON -> ADM found no failure
REASON -> ADM executed successful
RESULT -> ADM configure result in success
TGN ID -> ss7_tg2

Note  ID, CALL-AGENT-ID, TARGET-STATE, and MODE are required tokens for the control command.
Provisioning and Troubleshooting ISDN

Refer to the Cisco BTS 10200 Softswitch Release 3.5 ISDN Enhancements feature module for information on provisioning and troubleshooting ISDN.
Provisioning Analog Direct Inward Dial for PBXs

This chapter describes the steps required to activate analog direct inward dial (DID) to stations served by a Private Branch Exchange (PBX).

The Analog DID one-way feature allows incoming calls to a local PBX network to complete to a specific station without attendant assistance. The station address is provided by the Call Agent (CA) that controls an access gateway (AGW) connecting to the PBX. The number of digits to be outpulsed by the AGW to the PBX is configurable in the CA.

Figure 10-1 shows a typical application with a residential user (UserA) attempting to call a PBX user station (UserB). UserB is identified by a specific set of extension digits in the PBX. The Cisco BTS 10200 Softswitch uses Media Gateway Control Protocol (MGCP) signaling to communicate with the AGW, and controls the outpulsing of digits from the AGW to the PBX. A Foreign Exchange Office (FXO) board in the AGW uses Reverse Battery Signaling (per TIA/EIA-464B) to communicate with a DID trunk board in the PBX over an analog DID one-way trunk. When completing a call termination to the PBX:

1. The extension digits for UserB are outpulsed from the AGW toward the PBX.
2. The PBX receives the extension digits.
3. The PBX then completes the call to UserB.

Provisioning the AGW is not within the scope of this document. Refer to the AGW manufacturer’s documentation for those steps. For a complete list of CLI provisioning commands, refer to the Cisco BTS 10200 Command Line Interface Reference Guide.
To activate analog DID, perform the following steps.

**Note**
Use the **add** command when adding a new table ID to the database. Use the **change** command when modifying existing tokens.

**Step 1**
Add the MGW profile ID. Set the FXO token to Y (Yes) to indicate that the MGW has an FXO board.

```
add mgw-profile ID=fxo-mgp1; vendor=Cisco; silent-suppress-supp=y; mgcp-variant=none; 
  rbk-on-conn-supp=n; packet-type=ip; aal1=n; aal2=n; aal5=n; pvc=n; svc=n; ec=n; 
  mparty-conference=n; mparty-3way=n; num-per-mparty=1; num-of-mparty=1; lptime=10; 
  hptime=20; isdn=n; dtmf=y; mf=n; fxo=y; fxs=n; fgd=n; backhaul-type=rudp; 
  sdp-origfield-unsupp=y; sdp-sessname-unsupp=y; sdp-email-unsupp=y; sdp-phone-unsupp=y; 
  sdp-uri-unsupp=y; sdp-bandwidth-unsupp=y; sdp-info-unsupp=y; sdp-time-unsupp=y; 
  sdp-attrib-unsupp=y; mgcp-erqnt-unsupp=y; mgcp-hairpin-unsupp=y; mgcp-qloop-unsupp=y; 
  mgcp-3way-hshake-unsupp=n; mgcp-conn-id-at-gw-unsupp=y; mgcp-cmd-seq-unsupp=y; 
  port-start=1; description=fxo-testing;
```

**Step 2**
Add the MGW ID. Set the PBX token to Y to indicate that the MGW connects to a PBX.

```
add mgw id=2420_187; tsap-addr=10.89.227.187; call-agent-id=ca166; 
  mgw-profile-id=fxo_mgp1; status=oos; call-agent-control-port=0; mgw-backhaul-port=22; 
  call-agent-backhaul-port=33; rgw=y; tgw=n; nas=n; iad=n; pbx=y; ans=n; ivr=n;
```

**Step 3**
Add the channel-associated signaling (CAS) trunk group profiles. Use the type token to specify the type of CAS trunk group the AGW uses to communicate with the PBX.

```
add cas-tg-profile id=fxo-dtmf_im; type=dtmf-imstart; oss-sig=y; test-line=n; 
add cas-tg-profile id=fxo-dtmf_wink; type=dtmf-winkstart; oss-sig=y; test-line=n; 
add cas-tg-profile id=fxo-mf-im; type=mf-imstart; oss-sig=y; test-line=n; 
add cas-tg-profile id=fxo-mf-wink; type=mf-winkstart; oss-sig=y; test-line=n;
```

**Step 4**
Add the trunk group ID.

```
add trunk-grp id=151; call-agent-id=ca166; tg-type=cas; dial-plan-id=dp1; status=oos; 
  sel-policy=lru; direction=out; glare=odd; tg-profile-id=fxo-dtmf_im;
```

**Step 5**
Add the termination. Set the type token to **trunk**. Set the mgcp-pkg-type token to **dt** to indicate CAS dual tone multifrequency (DTMF) endpoints, or to **ms** to indicate CAS multifrequency (MF) endpoints.

```
add termination prefix=aaln/s1/; port-start=5; port-end=5; mgw-id=2420_187; type=trunk; 
  mgcp-pkg-type=dt; status=oos;
```

**Step 6**
Add the office code digit string. Set the did token to Y for a DID number. Provision the digit-string, office-code-index, and did tokens in the Office Code table as listed in **Table 10-1**.

```
add office-code digit-string=972-614; office-code-index=23; did=y;
```

**Step 7**
Add the route.

```
add route id=fxo-rt; lcr=Y; tgn1-id=151;
```

**Note**
You must add the route before adding a subscriber with term-type=route (next step).

**Step 8**
Add the subscriber. Set the policy-id to the ID of the route that was created in Step 7.

```
add subscriber id=fxo_sub1; category=pbx; name=fxo_sub1; status=active; privacy=none; 
  ring-type-dnl=1; ring-type-dn2=2; ring-type-dn3=3; billing-dn=972-614-0000; 
  term-id=aaln/s1/5; mgw-id=2420_187; tgn-id=151; usage-sens=n; sub-profile-id=dp1; 
  term-type=route; policy-id=fxo_rt;
```
Step 9  Add the trunk group. Set the main-sub-id to the ID of the main subscriber for this PBX.
*change trunk-grp id=151; call-agent-id=CA166; main-sub-id=fxo_sub1;*

Step 10 Add the trunk termination. Assign the tgn-id to the TG that was previously created.
*add trunk termination-prefix=aaln/S1/; termination-port-start=5; termination-port-end=5; cic-start=5; cic-end=5; tgn-id=151; mgw-id=2420_187;*

Step 11 Assign the termination to the trunk and TG that were previously created.
*change termination id=aaln/S1/5; mgw-id=2420_187; trunk-id=5; tgn-id=151;*

Step 12 Add the DN2 subscriber. The last four digits of the subscriber’s DN become the DN used by the serving CA. Note that, for purposes of call routing, a larger block of DNs takes precedence over any included smaller blocks. Therefore, do not set the DN token to a value that will impact other blocks, or individual DNs, that have already been provisioned.
*add dn2subscriber office-code-index=23; dn=xxxx; sub-id=fxo_sub1;*

**Caution**
Do not set the DN token to a value that will impact other blocks or individual DNs that are already provisioned. This can cause improper routing of calls. If a larger block of DNs is assigned to a PBX, the lower number of blocks or DNs becomes nonoperational. The system routes the calls to the PBX.

Step 13 Add the destination.
*add destination dest-id=fxo_dest; call-type=local; route-type=sub; zero-plus=n; intra-state=n; description=dn2subscriber_testing;*

Step 14 Add the dial plan.
*add dial-plan id=dp1; digit-string=972-614; reqd-digits=10; dest-id=fxo_dest;*

Step 15 Control the MGW in service.
*control mgw id=2420_187; mode=forced; target-state=ins;*

Step 16 Control the trunk group out of service.
*control trunk-grp id=151; call-agent-id=CA166; mode=forced; target-state=oos;*

Step 17 Control the trunk termination out of service.
*control trunk-termination trunk-grp-id=151; cic=5; mode=forced; target-state=oos;*

Step 18 Control the trunk group in service.
*control trunk-grp id=151; call-agent_id=CA166; mode=forced; target-state=ins;*

Step 19 Control the trunk termination in service.
*control trunk-termination trunk-grp-id=151; cic=5; mode=forced; target-state=ins;*
Table 10-1 describes how to provision the digit-string, office-code-index and did tokens for analog DID.

**Table 10-1  Provisioning the Digit String, Office Code Index and DID tokens in the Office Code and DN2Subscriber Tables**

<table>
<thead>
<tr>
<th>Number of DNs in a group supported by the PBX</th>
<th>Value to enter for DIGIT-STRING token&lt;sup&gt;1&lt;/sup&gt;</th>
<th>Value to enter for DID token&lt;sup&gt;2&lt;/sup&gt;</th>
<th>Token Used in Both Office Code and DN2Subscriber Table</th>
<th>Value to enter for OFFICE-CODE-INDEX token</th>
<th>Value to enter for DN token&lt;sup&gt;2&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>npa-nxx-xxx (last digit of DN omitted)</td>
<td>y</td>
<td>Index value for this digit string</td>
<td>nnnx</td>
<td>nnnx</td>
</tr>
<tr>
<td>100</td>
<td>npa-nxx-xx (last two digits of DN omitted)</td>
<td>y</td>
<td>Index value for this digit string</td>
<td>nxxx</td>
<td>nxxx</td>
</tr>
<tr>
<td>1,000</td>
<td>npa-nxx-x (last three digits of DN omitted)</td>
<td>y</td>
<td>Index value for this digit string</td>
<td>nxxx</td>
<td>nxxx</td>
</tr>
<tr>
<td>10,000</td>
<td>npa-nxx (last four digits of DN omitted)</td>
<td>y</td>
<td>Index value for this digit string</td>
<td>xxxx</td>
<td>xxxx</td>
</tr>
</tbody>
</table>

1. npa=area code for the specified office, nxx=exchange for the specified office, -xxx, -xx or -x (x=0...9) are additional numbers that apply to all stations served by the applicable PBX.
2. n=0...9, and x is the ASCII character x.
Provisioning Channel-Associated Signaling

This chapter provides the procedures necessary for provisioning, controlling, and troubleshooting channel-associated signaling (CAS) trunk groups on the Cisco BTS 10200 Softswitch and media gateways. This chapter contains the following sections:

- CAS Blocking, page 11-1
- Provisioning CAS Trunk Groups, page 11-2
- Media Gateway Setup for CAS, page 11-4
- CAS Trunk Group Control Commands, page 11-5
- Troubleshooting Procedures, page 11-7

The Cisco BTS 10200 Softswitch supports CAS signaling for CAS multifrequency (MF) and CAS dual tone multifrequency (DTMF) using the Media Gateway Control Protocol (MGCP). The MGCP on the Cisco BTS 10200 Softswitch supports MGCP MF for CAS MF, MGCP DT for CAS DTMF, and the MGCP MF operator package (MO) for Operator Services and 911.

The following start methods are supported for CAS:

- Immediate start
- Wink start

CAS Blocking

CAS blocking describes the behavior of the Cisco BTS 10200 Softswitch when a CAS trunk termination is manually controlled using the CLI to in-service (INS)/out-of-service (OOS). CAS blocking affects all CAS terminations.

The CAS trunk termination has one of the following administrative (admin) states, which you can change from the Cisco BTS 10200 Softswitch command-line interface (CLI):

- OOS
- INS
- UEQP
- MAINT

For example, you can execute the appropriate CLI command to change a trunk termination’s admin state from OOS to INS. For more details, refer to the Cisco BTS 10200 Command Line Interface Reference Guide.
When the CAS trunk termination’s admin state is either OOS or MAINT, the trunk is not available for the remote switch or PBX to use.

**MS Package**

An MS package is used for PBX DID/DOD trunks. To locally block CAS on these trunk terminations, control the trunk termination from INS to OOS. An RQNT (S: MS/bl) MGCP message is then sent to the gateway. To locally unblock CAS trunk terminations, control the trunk termination from OOS to INS. An RQNT (S: MS/rel; R: rlc) MGCP message is then sent to the gateway, and the CA then waits for the NTFY (O: MS/rlc) message.

**DT Package**

A DT package is used for DTMF and dial-pulse trunks. To locally block CAS on these trunk terminations, control the trunk termination from INS to OOS. An RQNT (S: DT/bl) MGCP message is then sent to the gateway. To locally unblock the CAS trunk terminations, control the trunk termination from OOS to INS. An RQNT (S: DT/rel; R: rlc) MGCP message is then sent to the gateway, and the CA then waits for the NTFY (O: DT/rlc) message.

**Provisioning CAS Trunk Groups**

To provision CAS trunk groups at the Cisco BTS 10200 Softswitch, you must provision the following tables in the order listed:

1. mgw-profile
2. mgw
3. cas-tg-profile
4. trunk-grp
5. termination
6. subscriber-profile (if the CAS trunk group will use a main subscriber)
7. subscriber (if the CAS trunk group will use a main subscriber)
8. trunk
9. Busy Line Verification (BLV) setup—For more information about BLV, refer to the *Cisco BTS 10200 Softswitch System Description Guide*.

Use the following steps to provision the CAS-specific data in the Cisco BTS 10200 Softswitch database. Referenced data tables, such as call agent, dial-plan, office-code, and so on, must already be provisioned. Additional commands are also necessary to provision routing and translation for CAS trunk groups (refer to the *Cisco BTS 10200 Command Line Interface Reference Guide*).

**Note**

Refer to the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide* for explanations of each token in the command. After entering each command, press the Return (Enter) key.

**Step 1**

Log in to the active Element Management System (EMS).
Perform the following steps on a console that can communicate using IP with the active EMS.

**Note** To verify which EMS is currently active, log in to any EMS or CA/FS machine as root user, and enter the `nodestat` command to display the IP address of the active EMS. Then exit.

1. Open a UNIX shell or XTerm window (or, in Windows, choose **Start>Run>Command Prompt**).
2. At the UNIX shell prompt, enter SSH and the IP address or domain name of the active EMS.
   ```
   ssh xxx.xxx.xxx.xxx
   ```
   The system responds with a login prompt.
3. Enter your username for access to the CLI session.
   ```
   <CLI username>
   ```
   The system responds with a password prompt.
4. Enter the password for the CLI username.
   ```
   <password for CLI username>
   ```
   The system responds with a CLI> prompt.

**Step 2** Add the media gateway profile and MGW.

a. Add the media gateway profile for the CAS gateway. For CAS MF, use `mf=y`. For CAS DTMF, use `dtmf=y`.
   ```
   add mgw-profile id=cas_mf; vendor=cisco; mgcp-version=mgcp_1_0; mparty-conference=n; mparty-3way=n; num-per-mparty=1; num-of-mparty=1; lptime=10; hptime=20; mf=y; sdp-origfield-unsupp=y; sdp-sessname-unsupp=y; sdp-email-unsupp=y; sdp-phone-unsupp=y; sdp-bandwidth-unsupp=y; sdp-info-unsupp=y; sdp-time-unsupp=y; sdp-ttrib-unsupp=y; mgcp-erqnt-unsupp=y; mgcp-hairpin-unsupp=y; mgcp-qloop-unsupp=y; mgcp-conn-id-at-gw-unsupp=y; port-start=1; rbk-on-conn-supp=n;
   ```

b. Add the MGW. Use the same MGW profile ID provisioned in Step 2a. Use the correct call agent control port as per your requirements. Set the trunking gateway to `tgw=y`.
   ```
   add mgw id=cas_gw_1; tsap-addr=c3810.161.ipclab.cisco.com; call-agent-id=CA146; mgw-profile-id=cas_mf; tgw=y;
   ```

**Step 3** Add the trunk group profile. Use `oss-sig=n` only if you are defining a CAS Operator Services trunk group (do not use `oss-sig=y` for 911 or E911 trunk groups or regular CAS trunk groups). Use `e911=n` only if defining a CAS trunk group to be used for E911.

   ```
   cas-tg-profile id=cas_mf_im; type=MF_IMSTART; oss-sig=n; test-line=n; e911=n;
   ```

**Step 4** Add the CAS trunk group.

   ```
   add trunk-grp id=4005; tg-type=CAS; dial-plan-id=dp1; sel-policy=LRU; direction=BOTH; glare=ODD; tg-profile-id=cas_mf_im; call-agent-id=CA166;
   ```

**Step 5** Add the CAS media gateway terminations.

   ```
   add termination prefix=DS1-0/; mgw-id=10.89.227.161; type=TRUNK; mgcp-pkg-type=MS; port-start=1; port-end=24;
   ```

**Step 6** Add a subscriber profile for the CAS main subscriber. This step is optional depending on whether a main subscriber is required for the CAS trunk group only for PBXs with the DT package. If this is not required, proceed to Step 8.
add subscriber-profile id=cas_sub_MF51; digit-map-id=default; dial-plan-id=dp1; local-pfx1-opt=NR; toll-pfx1-opt=NR; pop-id=1; ea-use-pic1=y;

Step 7  Add a subscriber and link the subscriber to the CAS trunk group. This step is optional depending on whether a main subscriber is required for the CAS trunk group. If this is not required, please proceed to Step 9.

add sub id=cas_mf_im_4005; category=pbx; name=cas4005; status=active; email=cas4005@ipcell.com; language=english; sip-url=sip_url; billing-dn=972-618-4005; dn1=972-618-4005; privacy=none; ring-type-dn1=1; tgn-id=4005; grp=n; usage_sens=n; sub-profile-id=cas_sub_mf51;

Step 8  Associate the subscriber with the CAS trunk group.

change trunk-grp id=4005; call-agent-id=CA166; main-sub-id=cas_mf_im_4005;

Step 9  Add the CAS trunk circuits. Use the termination information defined in Step 6.

add trunk cic-start=1; cic_end=24; tgn-id=4005; termination-prefix=DS1-0/; mgw-id=10.89.227.161; termination-port-start=1; termination-port-end=24;

[This completes the provisioning of the Cisco BTS 10200 Softswitch for CAS trunk groups. To bring a CAS trunk group into service after provisioning is completed, you must set up the MGCP media gateway and connect it by a T1 to a CAS PBX or its equivalent. You must apply the control commands to bring the trunk group in service at the EMS.

Media Gateway Setup for CAS

The Cisco BTS 10200 Softswitch must be connected to a media gateway supporting MGCP (MF, DT, and MO) using IP. Some examples of these media gateways are the Cisco MC3810, the Cisco C3660, and so forth. Contact Cisco TAC for additional details on gateways supported for CAS trunk groups.

Following is an example of the most relevant tokens for CAS trunk groups to configure in a Cisco MC3810 gateway. Enter the commands at the gateway configuration level prompt.

Note  For information on the procedures and commands you need to configure the gateway for CAS trunk groups, refer to the specific vendor gateway documentation.

You can use the mgp command (if it is supported) for setting up the gateway.

voice-card 0
controller T1 0
  mode cas
  framing esf
  clock source loop-timed
  linecode b8zs
ds0-group 0 timeslots 1-24 type e&m-immediate-start
voice-port 0:0
dial-type mf
dial-peer voice 1 pots
  application mgcpapp
  destination-pattern 1
  port 0:0

The controller type must be set to one of the following if you are provisioning the MS or DT packages:

• e&m-immediate-start
• e&m-wink-start

If you are provisioning for the MO package, set the controller type to fgd-os (used in the Cisco C3660 for Operator Services and 911 trunk groups). The voice-port dial-type default is DTMF. Use the dial-type mf when necessary to override this default.

**CAS Trunk Group Control Commands**

Once the CAS trunk group is provisioned in the Cisco BTS 10200 Softswitch and the corresponding MGCP gateway is configured for CAS, the MGW, the CAS trunk group and the CAS trunk circuits can be brought into service using the EMS control commands given in the following sections. This section includes the following subsections:

**Bring the Media Gateway In Service**

To bring a MGW in service, perform the following steps:

**Step 1** Control the MGW in service.

```
control mgw id=10.89.227.161; target-state=ins; mode=forced;
```

**Step 2** Verify the MGW status.

```
status mgw id=10.89.227.161;
```

Reply Example:

Reply :Success:Entry 1 of 1 returned.

MGW_ID -> cas_gw_1
RESULT -> ADM configure result in success
REASON -> ADM executed successful
ADMIN_STATE -> ADMIN_INS
OPER_STATE -> Media gateway in down status

**Bring the CAS Trunk Group In Service**

To bring a CAS trunk group in service, perform the following steps:

**Step 1** Control the trunk group in service.

```
control trunk-grp id=4005; target_state=ins; mode=forced;
```

**Step 2** Verify the trunk group status.

```
status trunk-grp id=4005;
```

Reply example:

```
TGN_ID -> 4005
RESULT -> ADM configure result in success
REASON -> ADM executed successful
ADMIN_STATE -> ADMIN_INS
OPER_STATE -> Trunk group in-service
```
Equi the CAS Trunk Terminations

To equip CAS trunk terminations, perform the following step:

**Step 1** Equip the trunk termination. This example equips all circuit identification codes (CICs) on the trunk termination.

```plaintext
equip trunk-termination tgn-id=4005; cic=all;
```

Bring the CAS Trunk Terminations In Service

To bring CAS trunk terminations in service, perform the following steps:

**Step 1** Control the trunk termination in service.

```plaintext
control trunk-termination tgn-id=4005; cic=all; mode=forced; target-state=ins;
```

**Step 2** Verify the trunk termination status.

```plaintext
status trunk-termination tgn-id=4005; cic=all;
```

Reply Example:


TGN_ID -> 4005
CIC -> 1
RESULT -> ADM configure result in success
REASON -> ADM executed successful
TERM_ADMIN_STATE -> ADMIN_INS
TERM_OPER_STATE -> Termination is idle
TERM_REASON -> No fault reason available
TRUNK_STATIC_STATE -> ACTV
TRUNK_DYNAMIC_STATE -> IDLE
TRUNK_REASON -> NON_FAULTY

TGN_ID -> 4005
CIC -> 2
RESULT -> ADM configure result in success
REASON -> ADM executed successful
TERM_ADMIN_STATE -> ADMIN_INS
TERM_OPER_STATE -> Termination is idle
TERM_REASON -> No fault reason available
TRUNK_STATIC_STATE -> ACTV
TRUNK_DYNAMIC_STATE -> IDLE
TRUNK_REASON -> NON_FAULTY
...

TGN_ID -> 4005
CIC -> 24
RESULT -> ADM configure result in success
REASON -> ADM executed successful
TERM_ADMIN_STATE -> ADMIN_INS
TERM_OPER_STATE -> Termination is idle
TERM_REASON -> No fault reason available
TRUNK_STATIC_STATE -> ACTV
TRUNK_DYNAMIC_STATE -> IDLE
TRUNK_REASON -> NON_FAULTY

Note
This status applies to all corresponding circuits in the CAS trunk group (for example, 1 to 24).

The CAS trunk group circuits are ready to originate and receive calls.

Troubleshooting Procedures

The following trunk terminations status example shows that the trunk terminations are ready to originate and receive calls, provided the MGW and trunk group are also in service.

TERM ADMIN STATUS -> ADMIN_INS
TERM OPER STATUS -> Termination is idle
CIC STATIC STATE -> ACTV
CIC DYNAMIC STATE -> IDLE

If the trunk termination does not show a TERM OPER STATUS of Termination is idle, then the media gateway is not responding properly to the Cisco BTS 10200 Softswitch request to come in service. Verify the following items to try to correct the problem:

1. Ensure that the tokens defined in the media gateway correspond to the tokens defined in the Cisco BTS 10200 Softswitch (for example, CAS MF immediate start).
2. Check that there are no alarms on the T1 connection between the media gateway and CAS PBX (must be in service). If the T1 is not in-service, verify the cable connection, and verify that the tokens in the media gateway correspond to the tokens in the CAS PBX (or other corresponding equipment). Check b8zs, esf, clock source (internal or loop-timed), and so forth.
3. Verify that the media gateway can communicate with the Cisco BTS 10200 Softswitch by pinging the Cisco BTS 10200 address from the gateway.
4. Verify that the Cisco BTS 10200 Softswitch can communicate with the media gateway by pinging the media gateway address.
5. Verify that the MGCP port defined in the MGW profile at the Cisco BTS 10200 Softswitch corresponds with the MGCP port defined at the media gateway.
6. Ensure that the T1 controller is not shut down (go to the controller level at the media gateway and execute the no shutdown command).
7. Ensure that the voice port is not shut down (go to the voice port level at the media gateway and execute the no shutdown command).
8. Ensure that MGCP is not shut down (go to the mgcp level at the media gateway and execute the no shutdown command).
9. Verify the status of the ports and circuits (execute the show voice port sum command at the media gateway).

The response to this command should be:
If the OPER STATUS is 'dorm', then the media gateway is up and ready. If OPER STATUS shows 'down', then go back to Steps 1 to 3 and 6 to 7 to correct the problem.

<table>
<thead>
<tr>
<th>IN</th>
<th>OUT</th>
<th>SIG-TYPE</th>
<th>ADMIN</th>
<th>OPER STATUS</th>
<th>STATUS</th>
<th>STATUS</th>
<th>EC</th>
</tr>
</thead>
<tbody>
<tr>
<td>0:0</td>
<td>1</td>
<td>e&amp;m-imd</td>
<td>1 up</td>
<td>dorm</td>
<td>idle</td>
<td>idle</td>
<td>y</td>
</tr>
</tbody>
</table>
Provisioning PacketCable

Refer to the *Cisco BTS 10200 Softswitch Release 3.5 PacketCable Feature Module* for information on provisioning PacketCable.
Provisioning Trunk Groups

This chapter describes how to provision trunk groups for the Cisco BTS 10200 Softswitch. Trunks connect one Call Agent to another Call Agent by using IP connections. The basic trunk group provisioning flow is shown in Table 13-1.

Table 13-1  Overview of Softswitch Trunk Group Provisioning

1. Add the softswitch trunk group profile.
2. Add the trunk group.
3. Add the route.
4. Add the route guide.
5. Add the destination.
6. Add the dial plan.
7. Control the trunk group into service.
8. Check the trunk group status.

For a detailed description of each table, command, and applicable tokens, refer to the Cisco BTS 10200 Softswitch Command Line Interface Reference Guide.

Provisioning Trunk Groups

To provision trunk groups on the Cisco BTS 10200 Softswitch, perform the following steps. The commands shown are typical, and must be adapted to your specific system.

Step 1  Add the softswitch trunk group profile.

```
add softsw-tg-profile id=XYZ_SS_PROFILE; protocol_type=sip-t;
```

Note  Use SIP-T if SS7/ISUP messages must be carried end-to-end to allow connection between the public switched telephone network (PSTN) network and the IP network. Use SIP if SS7/ISUP messages are not required.
Step 2  Add the trunk group. The trunk group table defines the type of trunks to use to reach an endpoint and its specific parameters.

```
add trunk-grp id=157; call-agent-id=CA123; tg-type=softsw;
softsw-tsap-addr=100.10.22.200:5060; tg-profile-id=XYZ_SS_PROFILE;
```

Step 3  Add the route. The Route table stores up to 10 trunk groups per route-id.

```
add route id=SS_RTE; tgn1_id=157;
```

Step 4  Add the route guide.

```
add route-guide id=SS_RTE_GUIDE; policy-type=ROUTE; policy-id=SS_RTE;
```

Step 5  Add the destination. The Destination table uses call type and routing type tokens to determine call routing for the dialed digits.

```
add destination dest-id=DEST2; route-type=ROUTE; route-guide-id=SS_RTE_GUIDE;
```

Step 6  [If not already done on your system, add a dial plan profile. Your local work order should indicate whether a new dial plan profile is needed.]

```
add dial-plan-profile id=BASIC_DPP;
```

Step 7  Add the dial plan. The Dial Plan table analyzes the NPA-NXX of dial digits, associates them with a dial plan ID, and determines the destination.

```
add dial-plan id=BASIC_DPP; digit-string=555; reqd-digits=7; dest-id=DEST2;
```

Step 8  Control the softswitch trunk group into service.

```
control trunk-grp id=157; call-agent-id=CA001; target-state=INS; mode=forced;
```

Step 9  Check the trunk group status.

```
status trunk-grp id=157;
```
Provisioning CALEA

This chapter provides the steps required to implement the Communications Assistance for Law Enforcement Act (CALEA) feature on the Cisco BTS 10200 Softswitch by a service provider. These steps are required to enable the CALEA feature.

Security

Anyone with a high enough command level can execute Electronic Surveillance commands. However, access can be more easily controlled using a work group. To set up a work group, the system administrator should log in as optiuser and execute the following set of commands:

**Step 1**
Create a workgroup for the ESS command.

```
change command-table noun=ess;verb=add;work-groups=<someWorkGroup>;
```

**Step 2**
Add this work group to the user who is authorized for CALEA.

```
change user name=<someUser>; work-groups=<someWorkGroup>;
```

CALEA has its own unique default username and password, assigned in the work-groups steps above. A user must now have both a high enough command level, and be in the work group, to execute CALEA commands. User login is by a Secure Shell (SSH) session. On the Cisco BTS 10200 Softswitch, the default password can only be reset by the system administrator. Perform the following steps to login and change the CALEA password.

**Step 1**
Log in.

```
ssh -l CALEA <IPaddress>
```

On the first SSH login, expect a message similar to:

```
The authenticity of host [hostname] can't be established.
Are you sure you want to continue connecting (yes/no)?
```

**Step 2**
Respond to the prompt.

```
yes
```
Press Enter. The password prompt appears. Enter the default CALEA password CALEA01. From this point on, all communications are encrypted.

**Step 3**
Change the password using the reset password command.

```
reset password name=<someuser>; newpassword=<newpassword>;
```

**Note**
See the Password Section in the Security Chapter of the Cisco BTS 10200 Softswitch Command Line Interface Reference Guide for more information about the password command.

---

### Service Independent Interception Provisioning

Perform the following steps to set up CALEA on the Cisco BTS 10200 Softswitch in an SII network. Example commands are provided, but may not replicate your specific network conditions.

**Step 1**
Enable SII using the Call Agent Profile table.

```
add call-agent-profile id=<CAid>; es-intercept-type=service-independent-intercept;
```

**Note**
The default value for es-intercept-type is packet-cable-intercept, so if your network is a PacketCable network, you do not have to set the es-intercept-type.

**Step 2**
Provision the Electronic Surveillance table. This identifies the delivery function (DF) server to the Cisco BTS 10200 Softswitch.

```
add ess cdc-df-address=<IPaddress>; cdc-df-port=<port#>
```

The CALEA feature is now available for use.

---

### PacketCable Electronic Surveillance Provisioning

Perform the following steps to set up CALEA on the Cisco BTS 10200 Softswitch in a PacketCable network. Example commands are provided, but may not replicate your specific network conditions.

**Step 1**
Enable PacketCable intercept using the Call Agent Profile table.

```
add call-agent-profile id=<CAid>; es-intercept-type=service-independent-intercept;
```

**Note**
The default value for es-intercept-type is packet-cable-intercept, so if your network is a PacketCable network, you do not have to set the es-intercept-type.

**Step 2**
Provision the Electronic Surveillance table using the following example. This identifies the delivery function (DF) server to the Cisco BTS 10200 Softswitch.

```
add ess cdc-df-address=<IPaddress>; cdc-df-port=<port#>
```
Step 3  Configure the other network elements in the network for CALEA support.

a. If a trunking gateway supports CALEA, and CALEA is enabled on the gateway, then, for the Media Gateway Profile table, set the mgcp-es-unsupp token.

   \texttt{change mgw-profile id=<mgw id>; mgcp-es-unsupp=n;}

b. If an Aggregation Router supports CALEA, and CALEA is enabled on the Aggregation Router, then:
   1.) Provision the Aggregation table.
   \texttt{add aggr id=<aggr id>; dqos-supp=n; es-supp=y}
   2.) In the Media Gateway table, add the aggr-id to all residential gateways associated to the Aggregation Router.
   \texttt{change mgw id=<mgw id>; aggr-id=er1}

\textbf{Note}  CALEA must be enabled on every trunking gateway, and aggregation router, used for CALEA. Consult your vendor documentation for instructions.

The CALEA feature is now available for use.

Refer to the \textit{Cisco BTS 10200 Command Line Interface Reference Guide} for command table and token descriptions.
Digit Manipulation

The Digit Manipulation (DIGMAN) feature provides the ability to modify the calling party number (also known as ANI (Automatic Number Identification)) and/or the called party number (also known as DNIS (Dial Number Information Service)) for both incoming and outgoing calls within the Cisco BTS 10200 Softswitch. In addition to modifying the calling number and the called number, the digit manipulation tables can also be used to modify the Nature of Address (NOA) of ANI and/or DNIS numbers.

When this document refers to ANI or DNIS manipulation, it includes both digit manipulation and NOA manipulation unless otherwise stated. When ANI manipulation is specified, it refers to the Calling Party Number (CPN) that is normally displayed when a call is terminated to a device with the Calling Number Delivery (CND) feature.

In countries like China, there are additional requirements regarding ANI display. The requirements are to display ANI in the “dialable” format. The term dialable means the user can simply call up the display and hit the dial button to place a return call based on the received ANI. This requires the ANI to contain the area code (NDC) for a long distance call, while only displaying Subscriber Number for a local call. The rules defined in this document can be used to manipulate ANI or DNIS digits to the desired format.

The Digit Manipulation (DIGMAN) feature provides several benefits over previous releases:

- Robust Dial Plans—NANP or E.164
- Flexible Call Processing
- ANI- or DNIS-based Routing

Specific restrictions applicable to various commands used with the DIGMAN feature are described in the Digit Manipulation Tables section.

The DIGMAN feature is not platform dependent. It is supported on any platform that has been certified as a host system for the Cisco BTS 10200 Softswitch.

The DIGMAN feature supports the following industry standards:

- North American Numbering Plan (NANP) – see http://www.nanpa.com/

There are no prerequisites associated with the implementation of the DIGMAN feature.

There are no configuration tasks associated with the implementation of the DIGMAN feature.
Overview

The following is an overview of what the digman tables provide for the Cisco BTS 10200 Softswitch.

Digit manipulation is performed based on as many as twenty different digit manipulation (digman) tables as designated by the digman-id and rule number, each of which can have a unique set of match-string and replace-string tokens and/or match-NOA and replace-NOA tokens.

The match-string is compared to the input-string. If a match is found, based on the rules specified here, then the replace-string replaces the matched string in all further call processing actions.

The match-string and replace-string tokens are constructed using the characters specified in Table 15-1.

Table 15-1  Digit Manipulation Rules—Match-String and Replace-String Characters

<table>
<thead>
<tr>
<th>Character(s)</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>digits 0 through 9, asterisk *, pound sign #</td>
<td>Valid for use at any position in the input-string token, match-string token, and replace-string token.</td>
</tr>
<tr>
<td>Caret (^)</td>
<td>Beginning of match-string character</td>
</tr>
<tr>
<td></td>
<td>The caret (^) can only be the first character in a match-string. If it appears at any other position in the match-string, an error is generated.</td>
</tr>
<tr>
<td></td>
<td>• If the caret (^) is the only character in the match-string, the input string is prefixed by the characters in the replace-string.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: input-string=9127210112; match-string=^; replace-string=011.</td>
</tr>
<tr>
<td></td>
<td>In this example, the digit string 011 is prefixed to the input-string. The resultant output-string=0119127210112.</td>
</tr>
<tr>
<td></td>
<td>• If other characters are also present in the match-string, the caret (^) indicates that matching characters at the beginning of the input-string are to be replaced by the characters in the replace-string.</td>
</tr>
<tr>
<td></td>
<td>The replace string does not have to be the same number of characters as the match-string; it can be a greater or a fewer number of characters.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: input-string=0119127210112; match-string=^011; replace-string=0122.</td>
</tr>
<tr>
<td></td>
<td>In this example, if the digit string 011 appears at the beginning of the input string, it will be replaced with the digit string 0122 in the replace-string. The resultant output-string= 01229127210112.</td>
</tr>
</tbody>
</table>

The following examples further illustrate the use of the caret (^) character:

• In this example, if the first character in the input-string is the prefix 1 it is removed and the remainder of the input-string is passed unaltered.

Enter input string 14692551234
Match string  ^1
Replace string none
MATCHED

Output string = 4692551234
Table 15-1  Digit Manipulation Rules—Match-String and Replace-String Characters (continued)

<table>
<thead>
<tr>
<th>Character(s)</th>
<th>Action</th>
</tr>
</thead>
</table>
| Caret (^), continued | - In this example, a 10-digit input-string (the dialed number) is converted to a 5-digit extension by removing the first six digits and replacing them with the number 5.  
  Enter input string 4692551234
  Match string ^469255
  Replace string 5
  MATCHED
  Output string = 51234  
- This example prefixes the specified digit(s) at the beginning of the input-string.  
  Enter input string 222
  Match string ^
  Replace string 1
  MATCHED
  Output string = 1222 |
| Dollar sign ($) | End of match-string character  
  The dollar sign ($) can only be the last (or only) character in a match-string. If it appears at any other position in the match-string, an error is generated.  
- If the dollar sign ($) is the only character that appears in the match-string, the characters in the replace-string are appended to the input-string.  
  **Example:** input-string=4692551234; match-string=$; replace-string=567.  
  In this example, the digits 567 from the replace-string are appended to the end of the input-string. The resultant output-string=4692551234567.  
- If the dollar sign ($) appears at the end of a match-string, the matching characters at the end of the input-string are replaced by the characters in the replace-string.  
  **Example:** input-string=4692551234; match-string=1234$; replace-string=0000.  
  In this example, the digits 0000 in the replace-string will replace the digits 1234 in the input-string. The resultant output string=4692550000.  
  The following examples further illustrate use of the dollar sign ($) character:  
- In this example, the dollar sign ($) coupled with the question mark (?) deletes the last four digits from the input-string regardless of what they are.  
  Enter input string 4692551234
  Match string ?????$  
  Replace string none
  MATCHED
  Output string = 469255 |
Overview

Dollar sign ($), continued

Adding a replace-string in this example replaces the last four digits in the input string with 0000 regardless of what the last four digits are.

Enter input string 4692551234
Match string ?????$
Replace string 0000
MATCHED

Output string = 4692550000

This example appends the specified digits (0000) to the input-string without deleting or replacing any characters in the input-string.

Enter input string 469255
Match string $
Replace string 0000
MATCHED

Output string = 4692550000

Dot (.)

The dot (.) character is a “don’t care” character that can appear at the beginning, the end, or both the beginning and end of a match-string.

It is used to identify the position of characters in the input-string that are disregarded during the matching operation.

• Dots (.), if specified, can appear as leading dots; trailing dots; or both.

  Examples: match-string=...555; match-string=555....;
  match-string=...555....;

• If the dot (.) character is the leading character(s) in the match-string, the corresponding position(s) at the beginning of the input-string is(are) disregarded.

  Example: match-string=...555

  indicates that “555” appears in positions 4 through 6 in the input-string and the matching operation does not care what characters are in digit positions 1 through 3.

  This match-string (“...555”) will produce a match on the input-string 4695551234, and the replace-string will replace the matched string.

• If the dot (.) character is the last character(s) in the match-string, the corresponding position(s) at the end of the input-string is(are) disregarded.

  Example: match-string=555....

  indicates that 555 precedes the last four characters in the input-string.

  This match string (555....) will also produce a match on the input-string 4695551234, and the replace-string will replace the matched string.

Table 15-1 Digit Manipulation Rules—Match-String and Replace-String Characters (continued)

<table>
<thead>
<tr>
<th>Character(s)</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dollar sign ($),</td>
<td>• Adding a replace-string in this example replaces the last four digits</td>
</tr>
<tr>
<td>continued</td>
<td>in the input string with 0000 regardless of what the last four digits</td>
</tr>
<tr>
<td></td>
<td>are.</td>
</tr>
<tr>
<td></td>
<td>Enter input string 4692551234</td>
</tr>
<tr>
<td></td>
<td>Match string ?????$</td>
</tr>
<tr>
<td></td>
<td>Replace string 0000</td>
</tr>
<tr>
<td></td>
<td>MATCHED</td>
</tr>
<tr>
<td></td>
<td>Output string = 4692550000</td>
</tr>
<tr>
<td>Dot (.)</td>
<td>• This example appends the specified digits (0000) to the input-string</td>
</tr>
<tr>
<td></td>
<td>without deleting or replacing any characters in the input-string.</td>
</tr>
<tr>
<td></td>
<td>Enter input string 469255</td>
</tr>
<tr>
<td></td>
<td>Match string $</td>
</tr>
<tr>
<td></td>
<td>Replace string 0000</td>
</tr>
<tr>
<td></td>
<td>MATCHED</td>
</tr>
<tr>
<td></td>
<td>Output string = 4692550000</td>
</tr>
</tbody>
</table>
Dot (.), continued

- In this example only input-strings with the digit “5” in positions 4, 5, and 6 will be matched; however, the ampersand (&) in the replace-string indicates if a match occurs the entire input-string is passed unaltered.

Enter input string    4695551234
Match string     ...555
Replace string &
MATCHED

Output string = 4695551234

- The replace-string “none” in this example indicates if the input-string has the digit “3” in positions 4 and 5, a match occurs and those two digits are deleted, but all other digits in the input-string are passed unaltered.

Enter input string    222333
Match string     ...33
Replace string none
MATCHED

Output string = 2223

The dot (.) character can also be used to check the length of the input string, as illustrated in the following example.

- In this example, if the input-string is 10-digits the ampersand (&) character in the replace-string indicates that the input-string should be passed unaltered.

Enter input string    4695551234
Match string          ..........  
  #CHECK IF INPUT STRING LENGTH=10
Replace string &
MATCHED

Output string = 4695551234
Overview

Question Mark (?) The question mark (?) can appear anywhere in a match-string as a “wildcard” character; however, multiple question marks (two or more) must be contiguous at the beginning or at the end of a match-string and not separated by any other character(s)—nor can they separate any other characters in a match-string.

- Question mark (?) character(s) can be used to match characters at the beginning or the end of the input-string.

  **Example:**
  
  match-string=???555

  indicates that the digits “555” must be preceded in the input-string by at least 3 digits.

  This match-string (“???555”) matches the input-string 4695551234. When a match is found, the replace-string will replace the matched string.

  **Example:** match-string=555????

  indicates that the digits “555” must be followed by at least 4 digits.

  This match-string (“555????”) matches the input-string 4695551234. When a match is found, the replace-string will replace the matched string.

- Question mark(s) (?), if specified, cannot appear between digits in a string.

  **Example:** Input-string=123456; or match-string=12??56; is invalid, but match-string=123???; or match-string ???456; is valid.

The following examples further illustrate the use of the question mark (?):

- In this example, the first four digits are deleted if the input-string begins with the digit “1.”

  Enter input string 14692551234
  Match string ^1???
  Replace string none
  MATCHED
  Output string = 2551234

- Here the first four digits are deleted regardless of what they are.

  Enter input string 4692551234
  Match string ????
  Replace string none
  MATCHED
  Output string = 469255

- This example replaces any three digits followed by “555” with a single digit “5.”

  Enter input string 4695551234
  Match string ???555
  Replace string 5
  MATCHED
  Output string = 51234

<table>
<thead>
<tr>
<th>Character(s)</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Question Mark (?)</td>
<td>The question mark (?) can appear anywhere in a match-string as a “wildcard” character; however, multiple question marks (two or more) must be contiguous at the beginning or at the end of a match-string and not separated by any other character(s)—nor can they separate any other characters in a match-string.</td>
</tr>
</tbody>
</table>

  - Question mark (?) character(s) can be used to match characters at the beginning or the end of the input-string.

    **Example:** match-string=???555

    indicates that the digits “555” must be preceded in the input-string by at least 3 digits.

    This match-string (“???555”) matches the input-string 4695551234. When a match is found, the replace-string will replace the matched string.

    **Example:** match-string=555????

    indicates that the digits “555” must be followed by at least 4 digits.

    This match-string (“555????”) matches the input-string 4695551234. When a match is found, the replace-string will replace the matched string.

  - Question mark(s) (?), if specified, cannot appear between digits in a string.

    **Example:** Input-string=123456; or match-string=12??56; is invalid, but match-string=123???; or match-string ???456; is valid.

The following examples further illustrate the use of the question mark (?):

- In this example, the first four digits are deleted if the input-string begins with the digit “1.”

  Enter input string 14692551234
  Match string ^1???
  Replace string none
  MATCHED
  Output string = 2551234

- Here the first four digits are deleted regardless of what they are.

  Enter input string 4692551234
  Match string ????
  Replace string none
  MATCHED
  Output string = 469255

- This example replaces any three digits followed by “555” with a single digit “5.”

  Enter input string 4695551234
  Match string ???555
  Replace string 5
  MATCHED
  Output string = 51234
## Overview

Ampersand (&) Prefix character that can only appear as the last character in a replace-string. The ampersand character (&) is used in the replace-string to leave the matched string as it is without replacing it with the replace-string.

- If the ampersand character (&) is specified by itself in a replace-string, it indicates that no digit manipulation is required on the matched string and the input-string should be left as it is. If a match occurs, it does confirm that the input-string matches the match-string.

**Example**: input-string=4695551234; match-string=...555....; replace-string=&;

The input-string matches the match-string; however, the replace-string is an ampersand character (&), which does not affect the replace-string but does return an indication of the match.

- If the ampersand character (&) is specified with other digits preceding it in a replace-string, the specified digits are prefixed to the matched string.

**Example**: input-string=4695551234; match-string=???555....; replace-string=1&;

The input-string is 10 digits long, and the digits in positions 4 through 6 are “555,” so the input-string is prefixed by the specified character(s). The resultant output-string=14695551234.

The following examples further illustrate use of the ampersand character (&):

- If the first three digits of the input-string are followed by the digits “255” in positions 4, 5, and 6, then the digit “1” is prefixed to the input-string.

  Enter input string 4692551234
  Match string ???255
  Replace string 1&
  MATCHED
  Output string = 14692551234

- This match-string is used to check if the input-string consists of a “1” followed by any 10 digits.

  Enter input string 14692551234
  Match string ^1........
  Replace string &
  MATCHED
  Output string = 14692551234

- This match-string checks if the input-string is 10 digits with digits “555” in positions 4, 5, and 6.

  Enter input string 4695551212
  Match string ^...555....
  Replace string &
  MATCHED
  Output string = 4695551212

<table>
<thead>
<tr>
<th>Character(s)</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ampersand (&amp;)</td>
<td>Prefix character that can only appear as the last character in a replace-string. The ampersand character (&amp;) is used in the replace-string to leave the matched string as it is without replacing it with the replace-string. If the ampersand character (&amp;) is specified by itself in a replace-string, it indicates that no digit manipulation is required on the matched string and the input-string should be left as it is. If a match occurs, it does confirm that the input-string matches the match-string. <strong>Example</strong>: input-string=4695551234; match-string=...555....; replace-string=&amp;; The input-string matches the match-string; however, the replace-string is an ampersand character (&amp;), which does not affect the replace-string but does return an indication of the match. If the ampersand character (&amp;) is specified with other digits preceding it in a replace-string, the specified digits are prefixed to the matched string. <strong>Example</strong>: input-string=4695551234; match-string=???555....; replace-string=1&amp;; The input-string is 10 digits long, and the digits in positions 4 through 6 are “555,” so the input-string is prefixed by the specified character(s). The resultant output-string=14695551234. The following examples further illustrate use of the ampersand character (&amp;): If the first three digits of the input-string are followed by the digits “255” in positions 4, 5, and 6, then the digit “1” is prefixed to the input-string. Enter input string 4692551234 Match string ???255 Replace string 1&amp; MATCHED Output string = 14692551234 This match-string is used to check if the input-string consists of a “1” followed by any 10 digits. Enter input string 14692551234 Match string ^1........ Replace string &amp; MATCHED Output string = 14692551234 This match-string checks if the input-string is 10 digits with digits “555” in positions 4, 5, and 6. Enter input string 4695551212 Match string ^...555.... Replace string &amp; MATCHED Output string = 4695551212</td>
</tr>
</tbody>
</table>
Chapter 15  Digit Manipulation

Digit Manipulation Tables

The Digit Manipulation Profile (digman profile) and the Digit Manipulation (digman) tables were added to the Cisco BTS 10200 Softswitch software to support digit manipulation in Release 3.3 V04. Prior to this release digit manipulation was accomplished in the dial plan table using `del_digits` and `pfx_digits`, but it was available only for the called party number (DNIS).

Digit manipulation can take place at several points in call processing, as illustrated in Figure 15-1:

- **Pre-translations**—In the pre-translations stage, the dial-plan-profile table is used to specify if ANI, DNIS or both are to be manipulated. The purpose of pre-translation stage is to normalize the digits as required during the translations stage. For example: if a region supports 7-digit dialing, you can use DNIS manipulation in the dial-plan-profile to add an HNPA (Home NPA) to make it a 10-digit DN.

- **Translations**—The dial-plan table can be used to manipulate the called party number (DNIS). Simple delete/prefix functionality is supported; however, this capability is no longer necessary.

### Table 15-1  Digit Manipulation Rules—Match-String and Replace-String Characters (continued)

<table>
<thead>
<tr>
<th>Character(s)</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (or none)</td>
<td>The word “None” (or “none”) can appear in either a match-string or a replace-string to specify a NULL string.</td>
</tr>
<tr>
<td></td>
<td>- If the word “None” (or “none”) appears in the match-string, it indicates when input-string is NULL, it should be replaced with the replace-string.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: input-string=NULL; match-string=none; replace-string=4692550000;</td>
</tr>
<tr>
<td></td>
<td>The input-string (NULL) matches the match-string (none), so the input-string is replaced by the replace-string (“4692550000”).</td>
</tr>
<tr>
<td></td>
<td>- If the word “None” (or “none”) appears in the replace-string, it indicates when a match occurs, the input-string should be replaced with NULL.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: input-string=4692551234; match-string=469255; replace-string=none;</td>
</tr>
<tr>
<td></td>
<td>A portion of the input-string matches the match-string, so the matched portion of the input-string is replaced with NULL (nothing). After the digit manipulation, the resultant string will be “1234.”</td>
</tr>
</tbody>
</table>
**Routing**—The Destination Table and/or Route Table can be used to specify digit manipulation of ANI, DNIS or both. The out-pulsing number can be normalized using the destination table. In addition, if special manipulation is required based on the route selected, then that can be specified with each Trunk Group within a route.

If the Called Party Number terminates within the Cisco BTS 10200 Softswitch, and the subscriber number points to a Trunk Group, then digit manipulation rules for ANI, DNIS, or both can be specified in the Trunk Group Table.

If the call is an interLATA call, or requires Carrier Routing, the ANI/DNIS digit manipulation IDs specified in the Destination table are ignored and carrier based routing is performed.

**Figure 15-2** illustrates the provisioning relationships for Cisco BTS 10200 Softswitch dial plans, which includes the ANI/DNIS digital manipulation functions described in this document.

The digman-profile table provides a digman-id that can be combined with up to 20 different match-string rules (one in each digman table) to be compared to the input-string. Each digman table is based on a unique combination of the digman-id and the rule number. When a digman table is found and both the match-string and replace-string are provisioned, the string manipulation function is invoked, which applies the match rule to the input-string. If there is a match to the rule, the replace-string replaces the match-string and the manipulated string is the resultant output-string.
When there is a digit string match, noa manipulation is also applied. If both match-noa and replace-noa are provisioned, and a match is obtained, the matched input-noa will be replaced with the replace-noa and the resultant noa is the output-noa.

The following sections describe the provisioning and actions in each of the three stages in greater detail.

**Pre-Translations Stage**

In the pre-translations stage, the dial-plan-profile table is used to specify if ANI, DNIS, or both are to be manipulated. The purpose of the pre-translation stage is to normalize the digits, as required, during the translations stage.

In addition to manipulating the ANI/DNIS digits, the pre-translation stage can also be used to determine the Nature of Address (NOA) of the incoming digits (either ANI or DNIS or both).

The Dial Plan Profile table has been modified to allow provisioning of the ANI and DNIS digit manipulation rules.

**Examples:**

- In the first example, since the first character of the input string matches the specified match-string (^*), the NOA is changed to a Vertical Service Code (VSC).

  Add digman id=pretrans; rule=1; match-string=^*; replace-string=&; match-noa=any; replace-noa=vsc;

  Enter input string *55#
  Match string ^*
  Replace string &
  MATCHED

  Output string = *55#

- In the second example, since the last character of the input string matches the specified match-string (#), the NOA is changed to a Vertical Service Code (VSC).

  Add digman id=pretrans; rule=2; match-string=#; replace-string=&; match-noa=any; replace-noa=vsc;

  Enter input string *55#
  Match string #
  Replace string &
  MATCHED

  Output string = *55#

- In the third example there is no match, so the NOA is not changed and the output-string is the same as the input-string.

  Add digman id=pretrans; rule=3; match-string=^*; replace-string=&; match-noa=any; replace-noa=vsc;

  Enter input string 5555
  Match string *
  Replace string &
  Not MATCHED

  Output string = 5555
Determining NOA for China

The following table can be used to determine the NOA of incoming calls for China.

<table>
<thead>
<tr>
<th>Rule #</th>
<th>Match-String</th>
<th>Replace-String</th>
<th>Match-NOA</th>
<th>Replace-NOA</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>*</td>
<td>&amp;</td>
<td>Any</td>
<td>VSC</td>
<td>If first digit is *, treat it as a VSC code.</td>
</tr>
<tr>
<td>2</td>
<td>#</td>
<td>&amp;</td>
<td>Any</td>
<td>VSC</td>
<td>If first digit is #, treat it as a VSC code.</td>
</tr>
</tbody>
</table>

Note

It is important to note that in North America the digman processing will not be available until after the hardcode parser is available. This means that all calls will be parsed and a NOA determined prior to performing the digman processing described in this document.

Digit Manipulation Profile Table

The Digit Manipulation Profile table is used to define an ID for the Digit Manipulation table. This ID is then used to specify a user-defined description for the corresponding Digit Manipulation table.

Table Name: DIGMAN-PROFILE
Table Containment Area: Call Agent
Command Line Actions: show, add, change, and delete
showdigman-profile id=ndc10;
adddigman-profile id=ndc10; description=Subscriber ANI digman id;
changedigman-profile id=ndc10; description=Subscriber ANI digman id;
deletedigman-profile id=ndc10;

Primary Key Token(s): ID
Add Rules: none
Change Rules: none
Delete Rules: FK restrictions

Table 15-3 Digit Manipulation Profile Table—Token Properties

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID—Digit Manipulation ID</td>
<td>PK</td>
<td>varchar(16)</td>
<td>1 – 16 ASCII characters</td>
<td>M</td>
</tr>
<tr>
<td>Description—A user specified</td>
<td></td>
<td>varchar(64)</td>
<td>1 – 64 ASCII characters</td>
<td>O</td>
</tr>
<tr>
<td>description that is associated with</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the Digit Manipulation ID.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Digit Manipulation Table

The Digit Manipulation Table is used to perform the actual digit and/or NOA manipulation. If a match is made between the input-string (or input-NOA) and the specified match-string (or match-NOA), the input-string (or input-NOA) is replaced by the match-string (or match-NOA).

Refer to the “Overview” section on page 15-2 for detailed information on the use of the match-string, replace-string, match-NOA, and replace-NOA tokens.

Table Name: DIGMAN
Table Containment Area: Call Agent
Command Line Actions: show, add, change, delete, and help

showdigman id=ndc10;
adddigman id=ndc10; rule=1; match-string=010; replace-string=123;
changedigman id=ndc10; rule=2; match-noa=any; replace-noa=subscriber;
deletedigman id=ndc10; rule=1;
helpdigman id

Primary Key Token(s): ID, RULE
Add Rules: if match-string ≠ NULL; then replace-string ≠ NULL;
if match-noa ≠ NULL; Then replace-noa ≠ NULL;
Change Rules: same as add rules
Delete Rules: none

Table 15-4 Digit Manipulation Table—Token Properties

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID—Digit Manipulation ID</td>
<td>PK, FK</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters</td>
<td>M</td>
</tr>
<tr>
<td>This is the ID assigned in the digman-profile table.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RULE—Used to specify the order in which the rules are applied.</td>
<td>PK</td>
<td>integer</td>
<td>1–20 (maximum)</td>
<td>M</td>
</tr>
<tr>
<td>MATCH-STRING—Used to match against the input-string.</td>
<td></td>
<td>varchar(40)</td>
<td>1–40 ASCII characters</td>
<td>O</td>
</tr>
<tr>
<td>Refer to the “Overview” section on page 15-2 for detailed information on match-string tokens.</td>
<td></td>
<td></td>
<td>Can be any of the following characters: Digits (0-9, *, #) Dot (.) Question Mark (?) Caret (^) Dollar Sign ($) Or the word “none”</td>
<td></td>
</tr>
<tr>
<td>REPLACE-STRING—If a match is found, the matched string is replaced with the replace-string.</td>
<td></td>
<td>varchar(40)</td>
<td>1–40 ASCII characters</td>
<td>O</td>
</tr>
<tr>
<td>Refer to the “Overview” section on page 15-2 for detailed information on replace-string tokens.</td>
<td></td>
<td></td>
<td>The characters can be any of the following: Digits (0-9, *, #) Ampersand (&amp;) Or phrase “none”</td>
<td></td>
</tr>
</tbody>
</table>
### Table 15-4  Digit Manipulation Table—Token Properties (continued)

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>MATCH-NOA—Used to match against the input-NOA.</td>
<td>varchar(16)</td>
<td>see list</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>MATCH-NOA Values:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ANY—Any NOA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ABBR—Abbreviated Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INTL—International Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NATIONAL—National Number (North America only)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NS0 through NS6 — Network specific (111 1000 — 111 1110)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPERATOR—Operator Call</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRIVATE—Private Numbering Plan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUBSCRIBER—Subscriber Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TEST-LINE—Test Line</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UNKNOWN—NOA is unknown.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VSC—Vertical Service Code</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REPLACE-NOA—If a match on the input-NOA is found, it is replaced with the NOA specified by this token.</td>
<td>varchar(16)</td>
<td>see list</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>REPLACE-NOA Values:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ANY—Any NOA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ABBR—Abbreviated Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INTL—International Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NATIONAL—National Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NS0 through NS6 — Network specific (111 1000 — 111 1110)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPERATOR—Operator Call</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRIVATE—Private Numbering Plan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUBSCRIBER—Subscriber Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TEST-LINE—Test Line</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UNKNOWN—NOA is unknown.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VSC—Vertical Service Code</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DESCRIPTION—User-assigned description for this digit manipulation table.</td>
<td>varchar(64)</td>
<td>1–64 ASCII characters</td>
<td>O</td>
<td></td>
</tr>
</tbody>
</table>
Dial Plan Profile Table

The Dial Plan Profile ID is assigned to a subscriber, an incoming trunk group, or a service provider. The Dial Plan Profile table provides the following functions:

- Define Pre-Translations table (if required)
- National Dial Plan ID
- International Dial Plan ID
- NOA-based Routing

Table Name: DIAL-PLAN-PROFILE
Table Containment Area: Call Agent
Command Line Actions: show, add, change, and delete

- show dial-plan-profile id=ndc10;
- add dial-plan-profile id=ndc10; nanp-dial-plan=n;
  dnis-digman-id=ndc10; ani-digman-id=ndc10;
  description=Dialing plan for ndc-10 Subscribers;
- change dial-plan-profile id=ndc10; ani-digman-id=ndc10;
- delete dial-plan-profile id=ndc10;

Primary Key Token(s): ID
Add Rules: none
Change Rules: none
Delete Rules:
- ID does not exist in any dial-plan::id.
- ID does not exist in any sub-profile::dial-plan-id.
- ID does not exist in any pop::lnp-dp-id.
- ID does not exist in any trunk-grp::dial-plan-id.
- ID does not exist in any carrier::dial-plan-id.

Table 15-5 Dial Plan Profile Table—Token Values

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID—Dial-plan-profile-id. Required before a dial plan can be provisioned.</td>
<td>PK</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>M</td>
</tr>
<tr>
<td>INTL-DIAL-PLAN-ID—Specifies which international dial plan ID to use with the dial plan ID. If this field is null, the Call Agent uses the default intl-dial-plan-id from the Call Agent Configuration table.</td>
<td>FK</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>NANP-DIAL-PLAN—Indicates if dial plan is in the North American Numbering Plan (NANP) format. If NANP dial plan is used, the EMS enforces the NANP rules—the digit string has to be in the format NXX-NXX-XXXX.</td>
<td>char(1)</td>
<td>Y/N (default = Y)</td>
<td></td>
<td>O</td>
</tr>
<tr>
<td>ANI-DIGMAN-ID</td>
<td>FK</td>
<td>digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
</tr>
<tr>
<td>DNIS-DIGMAN-ID</td>
<td>FK</td>
<td>digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
</tr>
</tbody>
</table>
Digit Manipulation Tables

International Dial Plan Profile Table

The International Dial Plan Profile (intl-dial-plan-profile) table is used to create unique IDs for international dial plans. An ID must be created before provisioning the International Dial Plan table.

- **Table Name:** INTL-DIAL-PLAN-PROFILE
- **Table Containment Area:** Call Agent
- **Command Line Actions:** show, add, change, and delete
  - `show intl-dial-plan-profile id=pop1;`
  - `add intl-dial-plan-profile id=pop1; description=Intl Dial plan;`
  - `change intl-dial-plan-profile id=pop1; description=default Intl Dial plan;`
  - `delete intl-dial-plan-profile id=pop1;`

**Primary Key Token(s):** ID

**Add Rules:** none

**Change Rules:** none

**Delete Rules:**
- ID does not exist in any dial-plan::id.
- ID does not exist in any sub-profile::dial-plan-id.
- ID does not exist in any pop::lnp-dp-id.
- ID does not exist in any trunk-grp::dial-plan-id.
- ID does not exist in any carrier::dial-plan-id.

### Table 15-5  Dial Plan Profile Table—Token Values (continued)

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT-DIAL-PLAN-ID—National Dial Plan ID to be used to retranslate dialed digits. This field is used only if dial-plan-id is different than dial-plan-profile id.</td>
<td>FK dial-plan-table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters. default = dial-plan-profile-id</td>
<td>O</td>
</tr>
<tr>
<td>DESCRIPTION—Allows the Service Provider to enter a dial-plan-profile description for identification purposes.</td>
<td>varchar(64)</td>
<td>1–64 ASCII characters.</td>
<td>O</td>
<td></td>
</tr>
</tbody>
</table>

### Table 15-6  Dial Plan Profile Table—Token Values

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID—International-dial-plan-profile-id. Required before an international dial plan can be provisioned.</td>
<td>PK</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>M</td>
</tr>
<tr>
<td>DESCRIPTION—Allows the user to enter an international-dial-plan-profile description for identification purposes.</td>
<td>varchar(64)</td>
<td>1–64 ASCII characters.</td>
<td>O</td>
<td></td>
</tr>
</tbody>
</table>
Translational Stage

The Dial-Plan table or International Dial-Plan table is used during the Translations stage to manipulate only the called party number. The previously existing capability of a simple delete and/or prefix digit manipulation function is supported.

Note: While the simple delete and/or prefix digit manipulation function is still supported, it is no longer necessary as the same function(s) can now be accomplished in the other two stages.

Dial Plan Table

Table Name: DIAL-PLAN
Table Containment Area: Call Agent
Command types include: show, add, change, and delete

- showdial-plan id=sub; digit-string=972-671;
- adddial-plan id=sub; digit-string=972-671; noa=national; dest-id=richardson;
- changedial-plan id=sub; digit-string=972-671; noa=national; dest-id=plano;
- deletedial-plan id=sub; digit-string=972-671; noa=national; dest-id=plano;

Primary Key Token(s): ID, DIGIT-STRING, NOA
Add Rules: None
Change Rules: None
Delete Rules: NOA token is required.

Table 15-7 Dial Plan Table—Token Values

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID — Dial Plan ID of Subscriber,</td>
<td>PK, FK</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters</td>
<td>M</td>
</tr>
<tr>
<td>Trunk Group, etc. as assigned by</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the Service Provider.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIGIT-STRING — Dialed digits (DNIS)</td>
<td>PK</td>
<td>varchar(14)</td>
<td>1–14 numeric characters</td>
<td>M</td>
</tr>
<tr>
<td>that was dialed)</td>
<td></td>
<td></td>
<td>entered as ndc-ec-dn</td>
<td></td>
</tr>
<tr>
<td>MIN-DIGITS — Minimum number of</td>
<td>smallint</td>
<td>range 1–26</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>digits required for a call.</td>
<td></td>
<td>default =10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note: When a fixed number of digits</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>are required, MIN-DIGITS = MAX-DIGITS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX-DIGITS — Maximum number of</td>
<td>smallint</td>
<td>range 1–26</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>digits allowed for a call.</td>
<td></td>
<td>(default = 10)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note: When a fixed number of digits</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>are required, MIN-DIGITS = MAX-DIGITS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 15-7  Dial Plan Table—Token Values (continued)

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOA—Nature of Address</td>
<td></td>
<td>varchar(16)</td>
<td>see list</td>
<td>O</td>
</tr>
</tbody>
</table>

**NOA Values:** (only three supported)
- NATIONAL—National Number
- SUBSCRIBER—Subscriber Number
- UNKNOWN—NOA is unknown.

<table>
<thead>
<tr>
<th>DEST-ID —Provides routing information for the dialed number. ID from the Destination table.</th>
<th>FK Destination table</th>
<th>varchar(16)</th>
<th>1–16 ASCII characters.</th>
<th>M</th>
</tr>
</thead>
</table>

| SPLIT-NPA— Automatically provisioned when a record is added to the split-NPA table. | | varchar(7) | see list | O |

**SPLIT-NPA Values:**
- OLD-NPA—Dialed number is associated with the old NPA.
- NEW-NPA—Dialed number is associated with the new NPA.
- NONE (Default)—Dialed number is not associated with split NPA.

<table>
<thead>
<tr>
<th>DEL-DIGITS—Specifies number of digits to be deleted from the input-string</th>
<th></th>
<th>smallint</th>
<th>0–16</th>
<th>O</th>
</tr>
</thead>
</table>

| PFX-DIGITS—Specifies the digits to be prefixed. | | varchar(16) | 1–16 numeric digits | O |
|------------------------------------------------ |---------------------|---------------------|-----|
### International Dial Plan Table

The Intl-Dial-Plan table holds International Dial Plan information for calls to regions outside the NANP. It contains the country code, minimum and maximum digits, the country name, and the route-grp-id.

**Table Name:** INTL-DIAL-PLAN  
**Table Containment Area:** Call Agent  
**Command Line Actions:** Show, add, delete, change, help

```plaintext
show intl-dial-plan id= default; cc=122;
add intl-dial-plan id= default; cc=122; min-digits=7; max-digits=10;
change intl-dial-plan id= default; cc=122; description=UK;
delete intl-dial-plan id= default; cc=122;
help intl-dial-plan;
```

**Primary Key Token(s):** ID; CC  
**Add Rules:** FK constraints  
**Change Rules:** FK constraints  
**Delete Rules:** FK constraints

#### Table 15-8 International Dial Plan Table—Token Values

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID—International Dial Plan ID</td>
<td>PK, FK</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>M</td>
</tr>
<tr>
<td>CC—Country Code digits as defined in ITU-T Recommendation E.164. Service Provider must determine and enter accordingly. Often found in the front of some telephone directories as well. Recommendation E.164 is available at <a href="http://www.int/publications/bookstore.htm">www.int/publications/bookstore.htm</a>.</td>
<td>PK</td>
<td>varchar(7)</td>
<td>1–7 numeric characters.</td>
<td>M</td>
</tr>
<tr>
<td>MIN-DIGITS—Minimum number of digits required for a call to this country. Minimum number of digits for any number in the country being added.</td>
<td>smallint</td>
<td>6–16 (Default=6)</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>MAX-DIGITS—Maximum number of digits allowed. Maximum number of digits for any number in the country being added.</td>
<td>smallint</td>
<td>6–16 (Default=16)</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>DEST-ID—Used only if the Service Provider is also a carrier and wants to route the international call to the appropriate gateway.</td>
<td>FK</td>
<td>varchar(16)</td>
<td>1–6 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>DESCRIPTION (EMS-only field)</td>
<td>varchar(64)</td>
<td>1–64 ASCII characters.</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Allows Service Provider to assign a description for identification purposes.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Routing Stage

The digit manipulations for an outgoing call can be performed using one of the following methods:

- Destination Table
- Route Table
- Trunk Group Table for subscriber termination

The ANI/DNIS digit manipulation specified in the Destination table is applied during the outgoing call setup. The out-pulsing number can also be normalized using the destination table. In addition, if special digit manipulation is required based on the route selected, it can be specified for each Trunk Group within a route.

If the called number terminates within the Cisco BTS 10200 Softswitch, and the subscriber number points to a Trunk Group, then digit manipulation rules for ANI, DNIS, or both can be specified in the Trunk Group table.

If the call is an interLATA call or requires Carrier routing (route-type=carrier), the ANI/DNIS digit manipulation IDs specified in the destination table are ignored and carrier based routing is performed.

**Note**

Although both `pfx_digits` and `del_digits` still work in the Cisco BTS 10200 Softswitch dial plan table, if the subscriber dials a 7-digit number, but LNP queries require a 10-digit DN, then the digman tables should be set up to add an NPA, making the called number a 10-digit DN before performing an LNP query.

Destination Table

The Destination Table is used to manipulate ANI digits, DNIS digits, or both for an outgoing call. The digits are manipulated at the ANALYZED_INFO PIC during the outgoing route selection process. If the destination ID indicates that the outgoing call is based on CARRIER ID, the ANI/DNIS digit manipulation is not performed and the call is routed based on the carrier data.

The Destination table is used to define the Call Type and the routing information for the dialed digits. Multiple digit strings in the Dial Plan Table can use the same destination id.

**Table Name:** DESTINATION

**Table Containment Area:** Call Agent

**Command Line Actions:** show, add, delete, change, help

```plaintext
show destination dest-id=DallasAustin;
add destination dest-id=DallasAustin; call-type=toll;
   route-type=route; route-guide-id=rg10;
change destination dest-id=DallasAustin; route-guide-id=rg11;
delete destination dest-id=DallasAustin;
help destination
```

**Number of instances:** 1,000

**Primary Key Token(s):** dest-id

**Add Rules:** If call-type=nas, then route-type=none

**Change Rules:** None

**Delete Rules:** id does not exist in any dial-plan::dest-id;
  id does not exist in any intl-dial-plan::dest-id;
### Table 15-9 Destination Table—Token Values

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEST-ID—Destination identification.</td>
<td>PK</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters</td>
<td>M</td>
</tr>
<tr>
<td>CALL-TYPE—Type of dialed call.</td>
<td>FK</td>
<td>varchar(9)</td>
<td>see list</td>
<td>O</td>
</tr>
</tbody>
</table>

**CALL-TYPE Values:**

- VACANT — Vacant code (default)
- TEST-CALL — Test call dialed as: 958/959-xxxx or 1xx
- INTL — International call
- LOCAL — Local call
- TOLL — IntraLATA toll call
- INTERLATA — InterLATA call (uses PIC or dialed CAC)
- NATIONAL — National Number. Use LSA table to determine if local, toll, or interLATA call
- TANDEM — Tandem call between Call Agent and next switch or Call Agent
- EMG — 911 calls.
- NON-EMG — 311 calls.
- DA — 411, NPA-555-1212 calls
- DA-TOLL — 1+411, 1+NPA-555-1212 calls
- REPAIR — 611 calls.
- RELAY — 711 calls.
- BUSINESS — 811- calls to business office
- TOLL-FREE — Toll free call (800, 888, 877, 866, 855, 8440)
- 900 — Service Access Code 900, use carrier to route call
- 500 — Service Access Code 500, use carrier to route call
- 700 — 700 SAC call, route via PIC or dialed CAC
- 976 — Information Services Calls
- TW — Time and Temperature Service
- INFO — Information Services Calls
- PREMIUM — Service Access Code 900, use carrier to route call
- PCS — Service Access Code 500, use carrier to route call
- NAS — Network Access Server
- POLICE — Police
- FIRE — Fire
- AMBULANCE — Ambulance
- TIME — Time
- WEATHER — Weather Report
- TRAFFIC — Traffic Accident Report
- LB-TEST — Loop Back Test Call (108 Test Line)
Table 15-9  Destination Table—Token Values (continued)

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROUTE-TYPE—Routing Type.</td>
<td></td>
<td>varchar(7)</td>
<td>see list</td>
<td>M</td>
</tr>
</tbody>
</table>

**ROUTE-TYPE Values:**
- **SUB**—Subscriber termination. Use office code index and last 4 digits of the DN to find the subscriber.
- **CARRIER**—Used for SAC calls. The call is routed based on the routing specified in the carrier table.
- **ROUTE**—Use route-guide for routing.
- **ANNC**—Use announcement-id to terminate call.
- **RID**—Use route id for routing.
- **DP**—Use Dial Plan ID to retranslate based on the new dial plan ID.
- **NONE**—No route required. Used for NAS application.

**CARRIER-ID**—*Carrier ID is required if route-type= CARRIER.
Call is routed to the specified carrier. Used for 900, 500 type calls and to route 800 calls to Access Tandem Server if Call Agent does not support 800 SCP query.
FK
Carrier table
char(4)
4 numeric characters: 0000 – 9999

**ROUTE-GUIDE-ID**—*Required if route-type=ROUTE.
FK
Route-Guide table
varchar(16)
1–16 ASCII characters.

**ROUTE-ID**—*Required if route-type=ROUTE.
FK
Route table
varchar(16)
1–16 ASCII characters.

**DIAL-PLAN-ID**—Dial Plan ID to be used to retranslate the dialed digits.
*Required if ROUTE-TYPE=DP
FK
varchar(16)
1–16 ASCII characters.

**GAP-ROUTING**—If set and GAP parameter is present, check if called number in the GAP parameter is a Call Agent PBX subscriber.
char(1)
Y / N
(default=N)

**ANNC-ID**—Announcement ID.
*Required if ROUTE-TYPE=ANNC.
smallint
1–1000

**ZERO-PLUS**—Specifies if 0+ calls are allowed.
char(1)
Y = 0+ calls are allowed to this destination (default)
N = 0+ calls are not allowed to this destination

**INTRA-STATE**—Specifies if dialed digits are for an intra-state (toll) destination.
char(1)
Y (Default) = intrastate
N = interstate
Digit Manipulation Tables

Table 15-9 Destination Table—Token Values (continued)

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNIS-DIGMAN-ID—DNIS (Called Party Number) digit manipulation ID.</td>
<td>FK digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>ANI-DIGMAN-ID—ANI (Calling Party Number) Digit Manipulation ID.</td>
<td>FK digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>DESCRIPTION (EMS-only field)—Allows Service Provider to enter a destination description for identification purposes.</td>
<td>varchar(64)</td>
<td>1–64 ASCII characters.</td>
<td>O</td>
<td></td>
</tr>
</tbody>
</table>

Route Table

The route table gives a list of up to 10 Trunk Groups to route a call. If all the Trunk Groups are either busy or not available, call processing uses alt-route-id (if specified) to route the call.

- If ANI/DNIS digman IDs are specified with selected trunk group, they are applied during routing.
- If DNIS digman ID is specified, the Delete Digits and Prefix Digits tokens are ignored.
- If Tech-prefix is to be pre-pended, it can be specified via the DNIS-DIGMAN-ID.

Table Name: ROUTE
Table Containment Area: Call Agent
Command Line Actions: show, add, change, delete, help

show route id=Dallas1;
add route id=Dallas1; tgn1-id=dallas-tg; prefix-digits1=972;
    del-digits1=0;
change route id=Dallas1; del-digits1=3;
delete route id=Dallas1;
help route

Primary Key Token(s): ID
Add Rules: FK constraints
Change Rules: FK constraints
Delete Rules: id does not exist in any <route-guide, policy-odr, policy-region, policy-percent, policy-tod, policy-prefix, policy-oli, or policy-pop>::policy-id where policy-type = route

Table 15-10 Route Table—Token Values

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID—Route identification.</td>
<td>PK</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>M</td>
</tr>
<tr>
<td>TG-SELECTION—Trunk Group Selection Policy</td>
<td>varchar(3)</td>
<td>see list</td>
<td></td>
<td>O</td>
</tr>
</tbody>
</table>

**TG-SELECTION Values:**
- LCR—Least Cost Routing
- RR—Round Robin
- SEQ—Sequential order (default)
- LS—Load Sharing
### Table 15-10 Route Table—Token Values (continued)

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALT-ROUTE-ID—Alternate Route ID used if all trunk groups in route are busy.</td>
<td>FK Route table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>CALL-AGENT-ID1—Home Call Agent ID for the dialed NPA or NPA-NXX</td>
<td>FK</td>
<td>varchar(8)</td>
<td>Not provisionable</td>
<td></td>
</tr>
<tr>
<td>TGN1-ID (or TG1)—First Trunk Group within the route. TGs are searched in the order specified unless LCR applies.</td>
<td>FK Trunk-grp table</td>
<td>integer</td>
<td>1–99999999</td>
<td>O</td>
</tr>
</tbody>
</table>

**Note** If LCR is applied, the Call Agent reads cost for each trunk group from the Trunk-grp table and selects trunks from the least expensive trunk group to the most expensive trunk group.

**Note** The TGN-ID field can also be provisioned by specifying TG instead of TGN-ID. The EMS does a lookup for TGN-ID based on the TG specified and provisions it.

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEL-DIGITS1—Number of digits to delete.</td>
<td>smallint</td>
<td>0–10</td>
<td>(Default = 0)</td>
<td>O</td>
</tr>
<tr>
<td>PFX-DIGITS1—Digits to be prefixed. Digits are prefixed after the number of specified digits are deleted.</td>
<td>varchar(10)</td>
<td>1–10 ASCII characters.</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>DNIS-DIGMAN-ID1—DNIS (Called Party) Digit Manipulation ID</td>
<td>FK digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>ANI-DIGMAN-ID1—ANI (Calling Party) Digit Manipulation ID</td>
<td>FK digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>CALL-AGENT-ID2—Home Call Agent ID for the dialed NPA or NPA-NXX</td>
<td>FK</td>
<td>varchar(8)</td>
<td>Not provisionable</td>
<td></td>
</tr>
<tr>
<td>TGN2-ID or (TG2)—Second Trunk Group within the route.</td>
<td>FK integer</td>
<td>1–99999999</td>
<td>O</td>
<td></td>
</tr>
</tbody>
</table>

**Note** The TGN-ID field can also be provisioned by specifying TG instead of TGN-ID. The EMS does a lookup for TGN-ID based on the TG specified and provisions it.

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEL-DIGITS2—Number of digits to delete.</td>
<td>smallint</td>
<td>0–10</td>
<td>(Default = 0)</td>
<td>O</td>
</tr>
<tr>
<td>PFX-DIGITS2—Digits to be prefixed for TGN2-ID. Digits are prefixed after number of specified digits are deleted.</td>
<td>varchar(10)</td>
<td>1–10 ASCII characters.</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>DNIS-DIGMAN-ID2—DNIS (Called Party) Digit Manipulation ID</td>
<td>FK digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>ANI-DIGMAN-ID2—ANI (Calling Party) Digit Manipulation ID</td>
<td>FK digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>CALL-AGENT-ID3—Home Call Agent ID for the dialed NPA or NPA-NXX</td>
<td>FK</td>
<td>varchar(8)</td>
<td>Not provisionable</td>
<td></td>
</tr>
<tr>
<td>TGN3-ID (or TG3)—Third Trunk Group within the route.</td>
<td>FK integer</td>
<td>1–99999999</td>
<td>O</td>
<td></td>
</tr>
</tbody>
</table>

**Note** The TGN-ID field can also be provisioned by specifying TG instead of TGN-ID. The EMS does a lookup for TGN-ID based on the TG specified and provisions it.
Table 15-10 Route Table—Token Values (continued)

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEL-DIGITS3—Number of digits to delete.</td>
<td>smallint</td>
<td>0–10 (Default = 0)</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>PFX-DIGITS3—Digits to be prefixed for TGN3-ID. Digits are prefixed after number of specified digits are deleted.</td>
<td>varchar(10)</td>
<td>1–10 ASCII characters.</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>DNIS-DIGMAN-ID3—DNIS (Called Party) Digit Manipulation ID</td>
<td>FK digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>ANI-DIGMAN-ID3—ANI (Calling Party) Digit Manipulation ID</td>
<td>FK digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>CALL-AGENT-ID4—Home Call Agent ID for the dialed NPA or NPA-NXX</td>
<td>FK</td>
<td>varchar(8)</td>
<td>Not provisionable</td>
<td></td>
</tr>
<tr>
<td>TGN4-ID (or TG4)—Fourth Trunk Group within the route.</td>
<td>FK</td>
<td>integer</td>
<td>1–99999999</td>
<td>O</td>
</tr>
</tbody>
</table>

Note: The TGN-ID field can also be provisioned by specifying TG instead of TGN-ID. The EMS does a lookup for TGN-ID based on the TG specified and provisions it.

| DEL-DIGITS4—Number of digits to delete. | smallint | 0–10 (Default = 0) | O |
| PFX-DIGITS4—Digits to be prefixed for TGN4-ID. Digits are prefixed after number of specified digits are deleted. | varchar(10) | 1–10 ASCII characters. | O |
| DNIS-DIGMAN-ID4—DNIS (Called Party) Digit Manipulation ID | FK digman-profile table | varchar(16) | 1–16 ASCII characters. | O |
| ANI-DIGMAN-ID4—ANI (Calling Party) Digit Manipulation ID | FK digman-profile table | varchar(16) | 1–16 ASCII characters. | O |
| CALL-AGENT-ID5—Home Call Agent ID for the dialed NPA or NPA-NXX | FK | varchar(8) | Not provisionable |
| TGN5-ID (or TG5)—Fifth Trunk Group within the route. | FK | integer | 1–99999999 | O |

Note: The TGN-ID field can also be provisioned by specifying TG instead of TGN-ID. The EMS does a lookup for TGN-ID based on the TG specified and provisions it.
### Table 15-10 Route Table—Token Values (continued)

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>TGN6-ID (or TG6)—Sixth Trunk Group within the route.</td>
<td>FK</td>
<td>integer</td>
<td>1–99999999</td>
<td>O</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The TGN-ID field can also be provisioned by specifying TG instead of TGN-ID. The EMS does a lookup for TGN-ID based on the TG specified and provisions it.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DEL-DIGITS6—Number of digits to delete.</td>
<td>smallint</td>
<td>0–10 (default = 0)</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>PFX-DIGITS6—Digits to be prefixed for TGN6-ID. Digits are prefixed after number of specified digits are deleted.</td>
<td>varchar(10)</td>
<td>1–10 ASCII characters.</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>DNIS-DIGMAN-ID6—DNIS (Called Party) Digit Manipulation ID</td>
<td>FK digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>ANI-DIGMAN-ID6—ANI (Calling Party) Digit Manipulation ID</td>
<td>FK digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>CALL-AGENT-ID7—Home Call Agent ID for the dialed NPA or NPA-NXX</td>
<td>FK</td>
<td>varchar(8)</td>
<td>Not provisionable</td>
<td></td>
</tr>
<tr>
<td>TGN7-ID (or TG7)—Seventh Trunk Group within the route.</td>
<td>FK</td>
<td>integer</td>
<td>1–99999999</td>
<td>O</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The TGN-ID field can also be provisioned by specifying TG instead of TGN-ID. The EMS does a lookup for TGN-ID based on the TG specified and provisions it.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DEL-DIGITS7—Number of digits to delete.</td>
<td>smallint</td>
<td>0–10 (Default = 0)</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>PFX-DIGITS7—Digits to be prefixed for TGN7-ID. Digits are prefixed the number of specified digits are deleted.</td>
<td>varchar(10)</td>
<td>1–10 ASCII characters.</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>DNIS-DIGMAN-ID7—DNIS (Called Party) Digit Manipulation ID</td>
<td>FK digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>ANI-DIGMAN-ID7—ANI (Calling Party) Digit Manipulation ID</td>
<td>FK digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>CALL-AGENT-ID8—Home Call Agent ID for the dialed NPA or NPA-NXX</td>
<td>FK</td>
<td>varchar(8)</td>
<td>Not provisionable</td>
<td></td>
</tr>
<tr>
<td>TGN8-ID (or TG8)—Eighth Trunk Group within the route.</td>
<td>FK</td>
<td>integer</td>
<td>1–99999999</td>
<td>O</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The TGN-ID field can also be provisioned by specifying TG instead of TGN-ID. The EMS does a lookup for TGN-ID based on the TG specified and provisions it.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DEL-DIGITS8—Number of digits to delete.</td>
<td>smallint</td>
<td>0–10 (default = 0)</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>PFX-DIGITS8—Digits to be prefixed for TGN8-ID. Digits are prefixed after specified number of digits are deleted.</td>
<td>varchar(10)</td>
<td>1–10 ASCII characters.</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>DNIS-DIGMAN-ID8—DNIS (Called Party) Digit Manipulation ID</td>
<td>FK digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
</tbody>
</table>
### Table 15-10 Route Table—Token Values (continued)

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANI-DIGMAN-ID8—ANI (Calling Party) Digit Manipulation ID</td>
<td>FK digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>CALL-AGENT-ID9—Home Call Agent ID for the dialed NPA or NPA-NXX</td>
<td>FK</td>
<td>varchar(8)</td>
<td>Not provisionable</td>
<td></td>
</tr>
<tr>
<td>TGN9-ID (or TG9)—Sixth Trunk Group within the route.</td>
<td>FK</td>
<td>integer</td>
<td>1–99999999</td>
<td>O</td>
</tr>
</tbody>
</table>

**Note** The TGN-ID field can also be provisioned by specifying TG instead of TGN-ID. The EMS does a lookup for TGN-ID based on the TG specified and provisions it.

| DEL-DIGITS9—Number of digits to delete. | smallint | 0–10 (default = 0) | O |
| PFX-DIGITS9—Digits to be prefixed for TGN9-ID. Digits are prefixed after specified number of digits are deleted. | varchar(10) | 1–10 ASCII characters. | O |
|DNIS-DIGMAN-ID9—DNIS (Called Party) Digit Manipulation ID | FK digman-profile table | varchar(16) | 1–16 ASCII characters. | O |
|ANI-DIGMAN-ID9—ANI (Calling Party) Digit Manipulation ID | FK digman-profile table | varchar(16) | 1–16 ASCII characters. | O |
|CALL-AGENT-ID10—Home Call Agent ID for the dialed NPA or NPA-NXX | FK | varchar(8) | Not provisionable | |
|TGN10-ID (or TG10)—Tenth Trunk Group within the route. | FK | integer | 1–99999999 | O |

**Note** The TGN-ID field can also be provisioned by specifying TG instead of TGN-ID. The EMS does a lookup for TGN-ID based on the TG specified and provisions it.

| DEL-DIGITS10—Number of digits to delete. | smallint | 0–10 (default = 0) | O |
| PFX-DIGITS10—Digits to be prefixed for TGN10-ID. Digits are prefixed after specified number of digits are deleted. | varchar(10) | 1–10 ASCII characters. | O |
|DNIS-DIGMAN-ID10—DNIS (Called Party) Digit Manipulation ID | FK digman-profile table | varchar(16) | 1–16 ASCII characters. | O |
|ANI-DIGMAN-ID10—ANI (Calling Party) Digit Manipulation ID | FK digman-profile table | varchar(16) | 1–16 ASCII characters. | O |
Trunk Group Table

The Trunk Group (trunk-grp) table identifies the trunk group and maps it to an associated Media Gateway.

Trunk Group based digit manipulation is applied only if the Trunk Group is retrieved as part of subscriber termination.

Table Name: TRUNK-GRP
Table Containment Area: Call Agent
Command Line Actions: show, add, change, delete, and help

- showtrunk-group id=101;
- add trunk-group id=101; call-agent-id=CA146; tg-type=ss7;
  dial-plan-id=tg-dp; dpc=101-55-103; tg-profile-id=SS71
- changetrunk-group id=101; cost=200;
- deletetrunk-group id=101;
- helptrunk-group

Primary Key Token(s): ID
Unique Index Token(s): softsw-tsap-addr

Add Rules: Carrier-id must exist in the carrier table; sub-id must exist in the subscriber table.

Change Rules: Ensure the sub-id exists in the Subscriber table, if entered; ensure the mgw-id exists in MGW table, if entered.

The DPC field cannot be changed.

Delete Rules: ID cannot exist in any subscriber::term-id; ID cannot exist in any trunk::term-id

ID cannot exist in any mlhg-terminal::term-id.

Trunk group status must be OOS.

TNS Rules:
If a call is interLATA, and going to an access tandem (AT), the TNS parameter is sent. This is also known as direct distance, or domestic dialing (DDD).

If a call is international, the TNS parameter is sent.

If a carrier ID is not assigned to a trunk group, the TNS parameter is sent.

If a carrier ID is assigned to a trunk group, the TNS parameter is not sent.

Table 15-11 Trunk Group Table—Token Values

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID—Trunk Group number.</td>
<td>PK</td>
<td>integer</td>
<td>1–99999999</td>
<td>M</td>
</tr>
<tr>
<td>TG —ASCII name for the Trunk Group.</td>
<td>UK</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters</td>
<td>O</td>
</tr>
<tr>
<td>CALL-AGENT-ID—Call Agent ID.</td>
<td>FK</td>
<td>varchar(8)</td>
<td>5 ASCII characters. Format CAAnnn where nnn=001 – 999. (3 char reserved for future use.)</td>
<td>M</td>
</tr>
</tbody>
</table>
### Table 15-11 Trunk Group Table—Token Values (continued)

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>TG-TYPE—Trunk Group Type.</td>
<td></td>
<td>varchar(6)</td>
<td>see list</td>
<td>M</td>
</tr>
<tr>
<td><strong>TG-TYPE Values:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ANNC—Announcement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOFTSW—Softswitch Trunk Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAS—Channel Associated Signaling</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISDN—Integrated Services Digital Network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SS7—SS7 Trunk Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H323—H323 Trunk Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NUM-OF-TRUNKS—This field is not provisionable; system generated value. EMS provisions this field when trunks are provisioned for the Trunk Group.</td>
<td>smallint</td>
<td>1–9999</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPC—Destination Point Code if SS7. *Required if tg-type=SS7. NOTE: The DPC cannot be modified by a CHANGE command.</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
<td>M*</td>
</tr>
<tr>
<td>SOFTSW-TSAP-ADDR—TSAP address of the remote Softswitch if TG type= SOFTSW or H323. Different ports should be used if multiple TGs to the same Softswitch are supported. *Required if tg-type=softsw or H323.</td>
<td>UK</td>
<td>varchar(64)</td>
<td>1–64 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>H323-GW-ID—Gateway ID to be used for this trunk group. *Required if tg-type = h323.</td>
<td>FK</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters</td>
<td>O</td>
</tr>
<tr>
<td></td>
<td>H323-GW table</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TG-PROFILE-ID—Trunk Group Profile. Optional only if tg type=annc.</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O*</td>
<td></td>
</tr>
<tr>
<td>STATUS—Service state. Service state is not provisionable. STATUS is only valid for the show command.</td>
<td>varchar(15)</td>
<td>see list</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>STATUS Values:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OOS—Out-of-Service (default)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAINT—Maintenance (Manual Override)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INS—in-Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OOS-PENDING—Waiting to go to OOS state. MAINT-PENDING—Waiting to go to MAINT state.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 15-11 Trunk Group Table—Token Values (continued)

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPER-STATUS—Operational Status</td>
<td>varchar(5)</td>
<td>see list</td>
<td>O</td>
</tr>
</tbody>
</table>

**OPER-STATUS Values:**
- NF—Non-Faulty (default)
- FA—Faulty
- NF-RB—Non-Faulty Remotely Blocked
- FA-RB—Faulty Remotely Blocked

**DIRECTION**—Direction of the TG. Incoming only, Outgoing only, or Both incoming and outgoing. If both incoming and outgoing, the GLARE parameter is required.

| DIRECTION | varchar(4) | see list | O |

**DIRECTION Values:**
- BOTH—Trunk group used for both incoming and outgoing calls (default)
- OUT—Used for outgoing calls only.
- IN—Used for incoming calls only.

**TRAFFIC-TYPE**—Indicates type of traffic carried over these trunk groups. This token is required for Incoming and Both-Way trunk groups. If not specified, the call agent shall default to LOCAL.

| TRAFFIC-TYPE | varchar(8) | see list | O |

**TRAFFIC-TYPE Values:**
- LOCAL—Local Incoming Trunk Group (default)
- TANDEM—Incoming Local / Tandem Trunk Group. Calls are allowed to Tandem through.
- PBX—not used

**SEL-POLICY**—Trunk Selection Policy. Rule: If ANNC type TG, use LRU as default.

| SEL-POLICY | varchar(4) | see list | O |

**SEL-POLICY Values:**
- ASC—Select trunks in ascending order. (default)
- DSC—Select trunks in descending order.
- ODD—Select only odd numbered trunks.
- EVEN—Select only even numbered trunks.
- LRU—Select least recently used trunk.
- MRU—Select most recently used trunk
- RAND—Select trunk randomly

**GLARE**—Used only in both-way trunks. Defines how to resolve a glare condition—a both-way simultaneous trunk seizure. Note: This field should be set to “ALL” for ISDN trunk groups.

| GLARE | varchar(5) | see list | O |

**GLARE Values:**
- SLAVE—All Slave (default)
- ALL—All Master
- ODD—Master odd numbered trunks.
- EVEN—Master even numbered trunks.
- PC—Point Code driven. Higher PC is the master. Allowed only if SS7 Trunk Group.

**ALT-ROUTE-ON-CONG**— Use alternate route on congestion.

| ALT-ROUTE-ON-CONG | char(1) | Y = SKIP | N = BLOCK (default) | O |
### Table 15-11 Trunk Group Table—Token Values (continued)

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIGNAL-PORTED-NUMBER—Used for LNP</td>
<td>char(1)</td>
<td>Y =</td>
<td>send IAM w/o GAP</td>
<td>O</td>
</tr>
<tr>
<td></td>
<td></td>
<td>N =</td>
<td>send IAM w/GAP (default)</td>
<td></td>
</tr>
<tr>
<td>COST—Relative cost value; used if LCR based TG selection is required.</td>
<td>smallint</td>
<td>0–999</td>
<td></td>
<td>O</td>
</tr>
<tr>
<td>POP-ID—Defines the number of POPs in a Call Agent; used for incoming Trunk Groups.</td>
<td>FK POP table</td>
<td>smallint</td>
<td>0–999</td>
<td>O</td>
</tr>
<tr>
<td>REGION—Region of the incoming Trunk Group.</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>DEL-DIGITS—Number of digits to delete.</td>
<td>smallint</td>
<td>0–14</td>
<td>(default = 0)</td>
<td>O</td>
</tr>
<tr>
<td>PFX-DIGITS—Digits to be prefixed.</td>
<td>varchar(10)</td>
<td>1–14 numeric digits</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNIS-DIGMAN-ID—DNIS (Called Party) Digit Manipulation ID</td>
<td>FK digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>ANI-DIGMAN-ID—ANI (Calling Party) Digit Manipulation ID</td>
<td>FK digman-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>CARRIER-ID—Carrier ID if direct Trunk Group to a carrier. Used during incoming call processing.</td>
<td>FK Carrier table</td>
<td>varchar(4)</td>
<td>Same as carrier-id in Carrier table.</td>
<td>O</td>
</tr>
<tr>
<td>SP-ID—Service Provider ID</td>
<td>FK Service provider table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>CAUSE-CODE-MAP-ID—represents the cause code received.</td>
<td>FK cause-code-map-profile table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>QOS-ID—Specifies QOS index to be used for codec selection.</td>
<td>FK QOS table</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td>REMOTE-SWITCH-LRN—LRN of the previous switch used for billing.</td>
<td>varchar(10)</td>
<td>NPA-NXX-XXXX</td>
<td>O</td>
<td></td>
</tr>
</tbody>
</table>
Digit Manipulation Tables

Table 15-11 Trunk Group Table—Token Values (continued)

<table>
<thead>
<tr>
<th>Token</th>
<th>PK/FK</th>
<th>Type</th>
<th>Values</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAIN-SUB-ID—Used for PBX subscribers.</td>
<td>FK</td>
<td>varchar(30)</td>
<td>1–30 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subscriber table</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIAL-PLAN-ID—Dial Plan ID to be used.</td>
<td>FK</td>
<td>varchar(16)</td>
<td>1–16 ASCII characters.</td>
<td>O</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dial Plan Profile table</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| ANI-BASED-ROUTING                  | char(1)| Y/N         | Y = If set, determine subscriber ID based on the ANI
                                           |       |             | N = Normal routing (default)     | O   |
| NO-ANSWER-TMR—Ring No Answer Timer | smallint | 0–300 seconds (Default = 185) | O   |
| CLLI—COMMON LANGUAGE→Location Identifier (CLLI™) for the remote switch. | char(11) | 11 ASCII characters | O   |
| DESCRIPTION—Allows the Service Provider to describe the Trunk Group for identification purposes. | varchar(64) | 1–64 ASCII characters. | O   |

1.COMMON LANGUAGE is a registered trademark and CLLI is a trademark of Telcordia Technologies.

Delete Digits Function

The Digit Manipulation (digman) table supports the following delete digit capabilities:

- Deletion of Leading Digits
- Deletion of Specific Leading Digits
- Deletion of Trailing Digits
- Deletion of Specific Trailing Digits
- Deletion of Leading Digits if Length Matches
- Deletion of Trailing Digits if Length Matches

The following sections provide examples of the Digit Manipulation (digman) table provisioning required to implement the functions listed above.
Deletion of Leading Digits

Add digman id=del3; match-string=???: replace-string=none; or
Add digman id=del3; match-string=???: replace-string=none;

Enter input string 4692551234
Match string ???
Replace string none
MATCHED

Output string = 2551234

********************************************************

Deletion of Specific Leading Digits

Add digman id=del00; match-string=^00; replace-string=none;

Enter input string 0012345
Match string ^00
Replace string none
MATCHED

Output string = 12345

*********************************************************************

Deletion of Trailing Digits

Add digman id=dellast4; match-string=????$; replace-string=none;

Enter input string 4692551234
Match string ????$
Replace string none
MATCHED

Output string = 469255

*********************************************************************

Deletion of Specific Trailing Digits

Add digman id=delx1212; match-string=1212$; replace-string=none;

Enter input string 4695551212
Match string 1212$
Replace string none
MATCHED

Output string = 469555

********************************************************************
Deletion of Leading Digits if Length Matches

Leading digits are deleted only if the length of the input-string matches the length of the match-string.

Add digman id=del110; match-string=^????..; replace-string=none; or
Add digman id=del110; match-string=???..; replace-string=none;

*******************************************************************************
Enter input string 4692551234
Match string ???........
Replace string none
MATCHED

Output string = 2551234
*******************************************************************************

Deletion of Trailing Digits if Length Matches

Trailing digits are deleted only if the length of the input-string matches the length of the match-string.

Add digman id=dellast4; match-string=......????; replace-string=none; or
Add digman id=del310; match-string=^......????$; replace-string=none;

*******************************************************************************
Enter input string 4692551234
Match string ......???
Replace string none
MATCHED

Output string = 469255
*******************************************************************************

Prefix Digits Function

The Digit Manipulation table also supports the prefixing of digits. The following prefix functions are supported:

- Prefixing Leading Digits
- Prefixing Leading Digits if Length Matches

The following sections provide examples of the Digit Manipulation (digman) table provisioning required to implement the two functions listed above.

Prefixing Leading Digits

Add digman id=pfx469; match-string=^; replace-string=469;
*******************************************************************************
Enter input string 5551234
Match string ^
Replace string 469
MATCHED

Output string = 4695551234
*******************************************************************************
Prefixing Leading Digits if Length Matches

Add digman id=pfx469if7; match-string="......."; replace-string=469;  or
Add digman id=pfx469if7; match-string=.......; replace-string=469;
*********************************************************************
Enter input string 5551234
Match string ^........
Replace string 469
MATCHED
Output string = 4695551234
*********************************************************************

Replace Digits Function

The Digit Manipulation table supports digit replacement based on matched string. When a match is found, the matched string is replaced with the replace-string.

- Replacing Leading Digits
- Replacing Trailing Digits
- Replacing Specific Digits
- Replacing Leading Digits if Length Matches
- Replacing Specific Digit Positions
- Replacing Specific Digits by Position
- Replace if Input String NULL

The following sections provide examples of the Digit Manipulation table provisioning required to implement the functions listed above.

Replacing Leading Digits

Add digman id=del6pfx5; match-string=??????; replace-string=5;  or
Add digman id=del6pfx5; match-string=??????; replace-string=5;
*******************************************************************
Enter input string 4692551234
Match string ?????
Replace string 5
MATCHED
Output string = 51234
*******************************************************************
Enter input string 4692551234
Match string ^????
Replace string 5
MATCHED
Output string = 51234
Replacing Trailing Digits

Add digman id=del4rep0000; match-string=????$; replace-string=0000;
******************************************************************************
Enter input string 4692551234
Match string????$
Replace string0000
MATCHED

Output string = 4692550000
******************************************************************************

Replacing Specific Digits

Add digman id=del469255pfx5; match-string=469255; replace-string=5;
******************************************************************************
Enter input string 4692551234
Match string469255
Replace string5
MATCHED

Output string = 51234
******************************************************************************

Replacing Leading Digits if Length Matches

Add digman id=del6pfx5; match-string=469255....; replace-string=5;
******************************************************************************
Enter input string 4692551234
Match string469255....
Replace string5
MATCHED

Output string = 51234
******************************************************************************
Enter input string 4692550
Match string469255....
Replace string5
Not MATCHED

Output string = 4692550
******************************************************************************

Replacing Specific Digit Positions

Add digman id=rep456w222; match-string=....???...; replace-string=222;
Add digman id=repplast4; match-string=.....???; replace-string=0000;
******************************************************************************
Enter input string 4695551234
Match string...???...
Replace string222
MATCHED

Output string = 4692221234
******************************************************************************
Enter input string 4695551234
Match string.....???
Replace string0000
MATCHED

Output string = 4695550000
******************************************************************************
Nature of Address (NOA) Manipulation

The Digit Manipulation table also supports Nature of Address (NOA) manipulation.

To perform NOA manipulation only, the match-string and the replace-string should both be NULL.

Add digman id=dg1; rule=1; match-noa=any; replace-noa=subscriber;

If both digit and NOA manipulation rules are defined, then digit manipulation is performed only if the NOA value specified in the match-noa token matches the input-noa and the value specified in the match-string token matches the input-string.

Add digman id=dg1; rule=1; match-string=%255; replace-string=5; match-noa=national; replace-noa=abbr;

Table 15-12 Nature of Address (NOA) Table

<table>
<thead>
<tr>
<th>NOA</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANY</td>
<td>When specified, matches any other NOA. This NOA can only be specified in the MATCH-NOA field</td>
</tr>
<tr>
<td>ABBR</td>
<td>Abbreviated number</td>
</tr>
<tr>
<td>INTL</td>
<td>International number</td>
</tr>
<tr>
<td>NATIONAL</td>
<td>National number</td>
</tr>
<tr>
<td>NS0</td>
<td>Network specific (111 1000) number</td>
</tr>
</tbody>
</table>
Table 15-12 Nature of Address (NOA) Table (continued)

<table>
<thead>
<tr>
<th>NOA</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS1</td>
<td>Network specific (111 1001) number</td>
</tr>
<tr>
<td>NS2</td>
<td>Network specific (111 1010) number</td>
</tr>
<tr>
<td>NS3</td>
<td>Network specific (111 1011) number</td>
</tr>
<tr>
<td>NS4</td>
<td>Network specific (111 1100) number</td>
</tr>
<tr>
<td>NS5</td>
<td>Network specific (111 1101) number</td>
</tr>
<tr>
<td>NS6</td>
<td>Network specific (111 1110) number</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPERATOR</td>
<td>an Operator Call</td>
</tr>
<tr>
<td>PRIVATE</td>
<td>Private Numbering Plan</td>
</tr>
<tr>
<td>SUBSCRIBER</td>
<td>Subscriber Number</td>
</tr>
<tr>
<td>TEST-LINE</td>
<td>Test Line Number</td>
</tr>
<tr>
<td>UNKNOWN</td>
<td>NOA is unknown</td>
</tr>
<tr>
<td>VSC</td>
<td>Vertical Service Code</td>
</tr>
</tbody>
</table>

Sample Provisioning

This section provides a sample provisioning script for the implementation of the digman functionality.

Figure 15-3 Sample Provisioning

Add `digman id=pretrans; rule=1; match_string=8807654321; replace_string=8881234;`

match_noa=any; replace_noa=unknown;

Add `dial-plan-profile ID=cdp20; description=china dial plan profile;`

nanp-dial-plan=N; ani-digman-id=ani_20; dnis-digman-id=pretrans;

Add `route id=rt_h323_id; lcr=n; tgn1-id=4092; del-digits1=0; del-digits2=0; del-digits3=0; del-digits4=0; del-digits5=0; del-digits6=0; del-digits7=0; del-digits8=0; del-digits9=0; del-digits10=0; tg-selection=seq; ani-digman-id1=dm_ani_add_0; dnis-digman-id1=dm_dnis_remove_0;`

Caller A, using dial-plan-id=cdp20, dials 8007654321. The call hits the dial-plan-profile table (1) and uses the pretrans entry (2 and 3). It matches on the 800 number (4) and replaces it with 8881234 (5).
Feature Interaction

In addition to the above, there is some feature interaction that you should be aware of. When a call is terminated to a subscriber with Call Forwarding activated, a feature interaction occurs when calls are forwarded out of the Cisco BTS 10200 Softswitch. In China, the Cisco BTS 10200 uses H323 signaling to route calls to the PSTN; however, this scenario applies to any call which is forwarded over a non-SS7 signaling interface.

The H323 protocol and other non-SS7 signaling protocols do not support the Charge Number parameter, Original Called Party Number, or Redirecting Party Number. When Call Forwarding occurs, the ANI manipulation is performed on the redirecting party number if it is available. The DN of the forwarding party should also be sent as ANI digits and, as such in a forwarding scenario, the called number of the forwarding party should also be manipulated for the call.

Glossary

Ampersand (&)—Replace-string character used to indicate that the matched string is to be left as-is without replacing it. It can only appear as the last character in a replace-string.

ANI—Automatic Number Identification. This is usually the calling party number (CPN).

Caret (^)—A match-string character used to indicate what characters at the beginning of the input-string are to be matched.

CND—Calling Number Delivery. Displays the calling number on telephones equipped to receive it.

DNIS—Dial Number Information Service. This is usually the called party number.

Dollar Sign ($)—A match-string character used to indicate what characters at the end of the input-string are to be matched.

Dot (.)—A “don’t care” character that can appear at the beginning, the end, or both the beginning and end of a match-string. Primarily used to indicate a character’s position in an input-string without regard to what that character may be. Can also be used to check the length of an input-string.

E.164 Numbering Plan—The international public telecommunication numbering plan.

Input-string—The set of characters presented to the DIGMAN function for manipulation. Can be either the ANI (calling number) or DNIS (called number) strings.

Match-string—Specifies the set of characters in the input-string that are to be matched. The matching action is dependent on the accompanying trigger(s) (Caret, Dot, Question Mark, Ampersand).


NDC—The area code in the North American Numbering Plan (NANP).

NOA—Nature of Address. Provides information about the nature of the called number.

NPA—Numbering Plan Area. (Part of the NANP)

Output-string—Set of characters produced as a result of the action(s) taken by the DIGMAN function.

PSTN—Public Switched Telephone Network.

Question Mark (?)—A “wildcard” character that can appear anywhere in a match-string. Multiple question marks (two or more) must be contiguous (not separated by any other characters) and they cannot separate any other characters in a match-string.

Replace-string—The set of characters that replace the match-string when a match occurs between the input-string and the match-string.
The Cisco BTS 10200 Softswitch provides a user interface for administering and monitoring the following internal system components:

- Call Agent (CA)
- Feature Server (FS)
- Element Management System (EMS)
- Bulk Data Management System (BDMS)

The softswitch components are always deployed in a dual active/standby configuration (side A and side B), with the two sides running on separate computers (hosts). The active instance of each host is backed up by standby instance of the other host. There is no traffic load sharing between the active and standby instances; the active instance performs all of the call processing, and the standby does none. At installation, side A is designated as primary and side B as secondary. In normal operation, the side designated primary runs in active mode and the side designated secondary runs in standby.

**States**

This section describes the returnable status and control states for the Cisco BTS 10200 Softswitch.

**Returnable Status States**

Status states can be in either Normal or Forced mode. Table 16-1 lists status state modes and definitions.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>INIT-NORMAL</td>
<td>Primary will be active, secondary will be standby; switchover allowed.</td>
</tr>
<tr>
<td>INIT-FORCED</td>
<td>Primary will be forced to active or standby, secondary will be forced to standby or active; no switchover allowed.</td>
</tr>
<tr>
<td>ACTIVE-NORMAL</td>
<td>Primary is active, secondary is standby; switchover allowed.</td>
</tr>
<tr>
<td>ACTIVE-FORCED</td>
<td>Primary or secondary has been forced to active; no switchover allowed.</td>
</tr>
</tbody>
</table>
## Table 16-1 Status State Modes and Definitions (continued)

<table>
<thead>
<tr>
<th>Mode</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>STANDBY-NORMAL</td>
<td>Primary should be active, secondary should be standby; switchover allowed.</td>
</tr>
<tr>
<td>STANDBY-FORCED</td>
<td>Primary or secondary has been forced to standby; no switchover allowed.</td>
</tr>
<tr>
<td>TRANSITION-TO-ACTIVE-NORMAL</td>
<td>Primary is going to active, secondary is going to standby; switchover allowed.</td>
</tr>
<tr>
<td>TRANSITION-TO-ACTIVE-FORCED</td>
<td>Primary has been forced to active or standby; secondary has been forced to standby or active; no switchover allowed.</td>
</tr>
<tr>
<td>TRANSITION-TO-STANDBY-NORMAL</td>
<td>Primary is going to standby, secondary is going to standby; switchover allowed.</td>
</tr>
<tr>
<td>TRANSITION-TO-STANDBY-FORCED</td>
<td>Primary has been forced to active or standby; secondary has been forced to standby or active; no switchover allowed.</td>
</tr>
<tr>
<td>N/A</td>
<td>Not a valid state.</td>
</tr>
<tr>
<td>FAULTY</td>
<td>Instance is not running, the other side is active if it is not faulty.</td>
</tr>
</tbody>
</table>
Returnable Control States

Control states can be in either Normal or Forced mode. Table 16-2 lists control state modes and definitions.

Table 16-2  Control States and Definitions

<table>
<thead>
<tr>
<th>State</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>NORMAL</td>
<td>Primary is active and secondary is standby.</td>
</tr>
<tr>
<td>FORCED-ACTIVE-STANDBY</td>
<td>Primary has been forced to active and secondary is standby.</td>
</tr>
<tr>
<td>FORCED-STANDBY-ACTIVE</td>
<td>Primary has been forced to standby and secondary is active.</td>
</tr>
</tbody>
</table>

Success and Failure Responses

One of the following messages is returned upon the success of a command:

- Reconfigured Successfully
- Already in this configuration

One of the following messages is returned upon the failure of a command:

- Mate Changeover Timeout
- Mate Refused Changeover
- If this command is executed it will cause a System Outage
- Invalid Configuration
- Local Changeover Timeout
- Local Changeover Failure

Status Application Command

The status application command allows a user to find out the state of any Cisco BTS 10200 Softswitch application (CA, FS, EMS, BDMS), including uptime, side indications, and additional qualifying reason information.

Use one of the following command examples to check the application status:

```
status application id=CA146;
status application id=CA146;
status application id=EM01;
status application id=EM01;
```

Control Application Command

The control application command allows a user to control the state of an application instance. This command takes the application specified either in service or out of service.

```
control application id=CA146; action=start
```

Note

This command will not work on a simplex system.
Call Agent

This section describes the status and control commands for the Cisco BTS 10200 Softswitch Call Agent.

Status Command

The status command reports the status of a Call Agent.

```
status call-agent id=CA146;
```

Reply Example:

```
Reply: Request was successful.
REPLY=CONFIGURATION COMMAND EXECUTED-> status call-agent
PRIMARY STATUS -> ACTIVE_NORMAL
SECONDARY STATUS -> STANDBY_NORMAL
```

Control Command

The control command puts the Call Agent into a specific mode (state).

```
control call-agent id=CA146; target-state=forced-standby-active;
call control call-agent id=CA146; target-state=forced-active-standby;
call control call-agent id=CA146; target-state=normal;
```

Reply Example:

```
Request was successful
REPLY=CONFIGURATION COMMAND EXECUTED->Reconfigured successfully.
```
Feature Server

This section describes the status and control commands for the Cisco BTS 10200 Softswitch Feature Server.

Status Command

The status command reports the status of a Feature Server.

```plaintext
status feature-server id=FSAIN205.Cisco.com;
```

Reply Example:

Request was successful.

REPLY=CONFIGURATION COMMAND EXECUTED-> status feature-server
PRIMARY STATUS -> ACTIVE-NORMAL
SECONDARY STATUS -> STANDBY-NORMAL

Control Command

The control command puts a Feature Server into a specific mode (state).

```plaintext
control feature-server id=FSAIN205.Cisco.com; target-state=normal;
```

Reply Example:

Request was successful

REPLY=CONFIGURATION COMMAND EXECUTED->control feature-server LOCAL STATUS

Element Management System

This section describes the status and control commands for the Cisco BTS 10200 Softswitch Element Management System (EMS). These commands are specific to the EMS. For Billing commands, see the “Bulk Data Management System” section on page 16-6.

Status Command

The status command reports the status of an EMS.

```plaintext
status element-manager id=EM01;
```

Reply Example:

Reply : Success:

ELEMENT MANAGER STATUS IS... ->
APPLICATION INSTANCE -> Element Manager [EM1]
PRIMARY STATUS -> ACTIVE NORMAL
SECONDARY STATUS -> FAULTY
EMS MYSQL STATUS IS ... -> Daemon is running!
ORACLE STATUS IS... -> Daemon is running!
Control Command

The control command puts an EMS into a specific mode (state).

```bash
control element-manager id=EM01; target-state=normal;
```

Reply Example:

Request was successful
REPLY=CONFIGURATION COMMAND EXECUTED->CONTROL EMS LOCAL STATUS

Bulk Data Management System

This section describes the status and control commands for the Cisco BTS 10200 Softswitch Bulk Data Management System (BDMS).

Status Command

The status command reports the status of the BDMS.

```bash
status bdms;
```

Reply Example:

Reply : Success:
BILLING SERVER STATUS IS... ->
APPLICATION INSTANCE -> Bulk Data Management Server [BDMS1]
PRIMARY STATUS -> ACTIVE_NORMAL
SECONDARY STATUS -> STANDBY NORMAL
BILLING MYSQL STATUS IS... -> Dameon is running!

Control Command

The control command puts the BDMS into a specific state (mode).

```bash
control bdms id=BDMS1; target-state=normal;
```

Reply Example:

Reply : Success:
APPLICATION INSTANCE -> Bulk Data Management Server [BDMS1]
REASON -> CONFIGURATION COMMAND EXECUTED->CONTROL BDMS LOCAL STATUS System
Status System

The status system command returns the status of all applicable components of the system, including the BDMS.

```
status system;
```

Reply Example:

```
Reply: Request was successful.
REPLY=CA146 Status is....
CONFIGURATION COMMAND EXECUTED -> status call_agent
PRIMARY STATUS -> ACTIVE_NORMAL
SECONDARY STATUS -> FAULTY

FSPTC235 Status is....
CONFIGURATION COMMAND EXECUTED -> status feature_server
PRIMARY STATUS -> ACTIVE_NORMAL
SECONDARY STATUS -> FAULTY

FSAIN205 Status is....
CONFIGURATION COMMAND EXECUTED -> status feature_server
PRIMARY STATUS -> ACTIVE_NORMAL
SECONDARY STATUS -> FAULTY

EM01 Status is....
CONFIGURATION COMMAND EXECUTED -> status billing_server
PRIMARY STATUS -> ACTIVE_NORMAL
SECONDARY STATUS -> STANDBY_NORMAL

EM01 Status is....
CONFIGURATION COMMAND EXECUTED -> status element_manager
PRIMARY STATUS -> ACTIVE_NORMAL
SECONDARY STATUS -> FAULTY

MYSQLD Status is....
MYSQL dameon is running -> ACTIVE

ORACLE Status is....
ORACLE dameon is running -> ACTIVE
```
Maintenance and Diagnostics: External Resources

Administration and maintenance commands control or show the status of an external resource. The commands described in this chapter are specific to, and listed under, the applicable type. Sample responses, replies, and failure reasons are also listed in this chapter.

The Cisco BTS 10200 Softswitch monitors and administers resource states, and accesses the following external resources:

- Aggregation routers
- Media gateways (MGWs), including the following gateway types:
  - Residential gateways (RGWs)
  - Integrated access devices (IADs)
  - Trunking gateways (TGWs)
  - Network access servers (NAS)
- Trunk groups (TGs)
- Trunks
- Subscriber terminations

The following resources have dependencies:

- Allowed subscriber states depend upon the current RGW or IAD state.
- Allowed trunk states for ISDN depend upon the current TG state, which in turn depends upon the current TGW state.
- Allowed trunk states depend upon the TGW.

There are two types of service states for MGW, TG, and subscriber terminations:

- Administrative—The state that the Softswitch operator has provisioned for the resource
- Operational—The physical condition of the resource

These two types of service states are independent of each other. This is illustrated with the following example:

A Cisco BTS 10200 Softswitch operator executes the control command to place an MGW connection in service. The administrative state is now “In Service” (ADMIN_INS). However, the link between the Softswitch and the MGW might be out (cut, damaged, or placed out of service by the owner/operator of
Aggregation Status

This section details the status command for an aggregation (aggr) router. Aggregation routers are used in cable and network-based call signaling (NCS) markets. In cable markets, they are used as cable modem termination systems (CMTSs). In NCS markets, they are used as edge routers.

**Step 1**

Use the following example to check the status of an aggregation router:

```
status aggr id=CMTS1
```

Reply Example:

```
Reply : Success:
AGGR ID -> CMTS1
OPER STATE -> AGGR IN Service
RESULT -> ADM configure result in success
REASON -> ADM executed successful
```

The following list provides the AGGR operational-state values and possible responses for the command:

1. **IN SERVICE**
   - a. Means the TCP connection to the AGGR is up.
   - b. CLI output: AGGR IN SERVICE.

2. **CONNECTING**
   - a. Means the TCP connection to the AGGR is being set up.
   - b. CLI output: AGGR CONNECTING.

3. **INITIALIZING**
   - a. Identifies the initial state of the AGGR before a Call Agent (CA) attempts to connect to it.
   - b. CLI output: AGGR INITIALIZING (this is a transitional state, which a user may rarely see).

4. **OUT OF SERVICE**
   - a. Means the AGGR is out of service.
   - b. CLI output: AGGR OUT OF SERVICE.

ISDN Switchover

This section describes the control command for ISDN switchover. For ISDN status, use the status trunk group command described in the “Trunk Group” section on page 17-4. This command is only applicable to nonfacility-associated signaling (NFAS). It switches the D channel that is active to standby, and the D channel that is standby to active.

**Step 1**

Use the following example to switch over an ISDN D channel.
control isdn-dchan tgn-id=1;

Reply Example:
Reply : Success

Media Gateway

This section describes the Administration, Diagnostic, and Maintenance (ADM) status and control commands for media gateways.

Status Command

This section describes how to check the status of a media gateway.

**Step 1**
The following example checks the status of a media gateway:

`status mgw id=c5300_197;`

Reply Example:
Reply : Success:

MGW ID -> c5300_197
RESULT -> ADM configure result in success
REASON -> ADM executed successful
ADMIN STATE -> ADMIN_INS
OPER STATE -> Media gateway in working status

Table 17-1 lists the administrative states the system can return.

<table>
<thead>
<tr>
<th>State</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMIN-INS</td>
<td>In Service.</td>
</tr>
<tr>
<td>ADMIN-OOS</td>
<td>Out of Service.</td>
</tr>
<tr>
<td>ADMIN-MAINT</td>
<td>Maintenance Mode.</td>
</tr>
<tr>
<td>ADMIN-OOS-PENDING</td>
<td>Transitioning to Out of Service.</td>
</tr>
<tr>
<td>ADMIN-MAINT-PENDING</td>
<td>Transitioning to Maintenance Mode.</td>
</tr>
</tbody>
</table>

Control Command

This section shows how to control a media gateway in service. Modes can be either forced or graceful. Forced mode tears down all calls immediately; graceful mode allows calls in progress to complete before teardown.

**Step 1**
Use the following example to control a media gateway in service:

`control mgw id=c5300_162; mode=forced; target-state=INS;`
Reply Example:
Reply : Success: CLI change successful
MGW ID -> c5300_162
INITIAL STATE -> ADMIN_OOS
REQUEST STATE -> ADMIN_INS
RESULT STATE -> ADMIN_INS
FAIL REASON -> ADM found no failure
REASON -> ADM executed successful
RESULT -> ADM configure result in success

Note: The rules for placing an MGW into the OOS, INS, and MAINT states are shown in Figure 17-1.

Figure 17-1  Administrative and Operational Maintenance States for MGW

Trunk Group
This section describes the ADM status and control commands for trunk groups.
Status Command

This section describes how to show the status of one trunk group ID.

---

**Step 1**

The following example shows the status of a single trunk group ID:

```bash
status trunk-grp id=2;
```

Reply Example:

```
RESULT -> ADM configure result in success
REASON -> ADM executed successful
ADMIN STATE -> ADMIN_INS
OPER STATE -> Trunk group in-service
TGN ID -> 2
```

---

Table 17-2 lists the administrative states the system can return.

**Table 17-2  Returnable Administrative States**

<table>
<thead>
<tr>
<th>State</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMIN-INS</td>
<td>In Service.</td>
</tr>
<tr>
<td>ADMIN-OOS</td>
<td>Out of Service.</td>
</tr>
<tr>
<td>ADMIN-MAINT</td>
<td>Maintenance Mode.</td>
</tr>
<tr>
<td>ADMIN-OOS-PENDING</td>
<td>Transitioning to Out of Service.</td>
</tr>
<tr>
<td>ADMIN-MAINT-PENDING</td>
<td>Transitioning to Maintenance Mode.</td>
</tr>
</tbody>
</table>

The system can return the following operating states:

- Trunk group in-service
- Trunk group out-of-service
- Trunk group manually busy
- Trunk group operate in wait state
- Trunk group operate in standby state
- Trunk group restore session request normal
- Trunk group restore session request switch-over
- Trunk group restore session request maintenance
- Trunk group restore session fail normal
- Trunk group restore session fail switch-over
- Trunk group restore session fail maintenance
- Trunk group restore establish request normal
- Trunk group restore establish request switch-over
- Trunk group restore establish request maintenance
- Trunk group restore establish fail normal
- Trunk group restore establish fail switch-over
Aggregation Status

- Trunk group restore establish fail maintenance
- Trunk group in maintenance state
- Trunk group down session set fail soft normal
- Trunk group down session set fail hard normal
- Trunk group down session set fail soft maintenance
- Trunk group down session set fail hard maintenance
- Trunk group down establish request soft normal
- Trunk group down establish request hard normal
- Trunk group down establish request soft maintenance
- Trunk group down establish request hard maintenance
- Trunk group down establish fail soft normal
- Trunk group down establish fail hard normal
- Trunk group down establish fail soft maintenance
- Trunk group down establish fail hard maintenance
- Trunk group down establish request soft normal
- Trunk group down establish request hard normal
- Trunk group down establish fail soft normal
- Trunk group down establish fail hard normal
- Trunk group delete graceful
- Trunk group request remove release
- Trunk group request remove session set
- Trunk group remove graceful in-service and maintenance state
- DPC is inaccessible

The following states are available as of Release 3.5.3:

- ACL congestion is at level 1
- ACL congestion is at level 2
- ACL congestion is at level 3
- TFC congestion is at level 1
- TFC congestion is at level 2
- TFC congestion is at level 3

Control Command

This section describes how to control one trunk group ID.

Note

In Release 3.5, when performing the following commands in immediate succession, always wait at least one second before performing the second command:

control trunk-grp tgn-id=129; mode=forced; target-state=oos;
control trunk-grp tgn-id=129; mode=forced; target-state=ins;

Step 1

The following example controls a single trunk group ID into service:

c ontrol trunk-grp id=2; mode=forced; target-state=INS;

Reply Example:
Subscriber Termination

This section describes the status and control commands for subscriber terminations. Either a range of subscribers can be specified by using *@mgw-id for the ID parameter, or a single subscriber can be specified (for example: sub-ctx1@Cisco.com).

When first provisioned, all subscriber terminations are in the unequipped (UEQP) state. A subscriber termination must also be in the UEQP state before it can be deleted.

Individual subscriber terminations can be placed into any of three administrative service states: INS, OOS, and MNT. The relationship between subscriber termination states and the residential gateway (RGW) state is provided in Table 17-3.

Table 17-3 RGW/IAD and Subscriber Termination States

<table>
<thead>
<tr>
<th>RGW/IAD State</th>
<th>Allowed Subscriber Termination States</th>
</tr>
</thead>
<tbody>
<tr>
<td>OOS</td>
<td>• OOS</td>
</tr>
<tr>
<td></td>
<td>• UEQP</td>
</tr>
<tr>
<td>INS</td>
<td>• OOS</td>
</tr>
<tr>
<td></td>
<td>• MAINT</td>
</tr>
<tr>
<td></td>
<td>• INS</td>
</tr>
<tr>
<td></td>
<td>• UEQP</td>
</tr>
<tr>
<td>MAINT</td>
<td>• OOS</td>
</tr>
<tr>
<td></td>
<td>• MAINT</td>
</tr>
<tr>
<td></td>
<td>• UEQP</td>
</tr>
</tbody>
</table>

where:
• RGW—residential gateway
• IAD—integrated access device
• OOS—out of service

Caution
When you control an ISDN trunk in-service, the media gateway must be in-service. When you control an ISDN trunk group, all ISDN trunks in that trunk group are controlled to the same state.
- MAINT—maintenance
- INS—in service
- UEQP—unequipped

The rules for placing RGW and IAD subscriber terminations into the OOS, INS, and MAINT states (which depend upon the RGW or IAD state) are shown in Figure 17-2.
Figure 17-2 Administrative and Operational Maintenance States for Residential Gateways

- If SL = NE
  - SL = UEQP
  - Add (SL)*
  - Del (SL)*
  - If SL = UEOQP Del (SL)

- If SL = OOS
  - SL = NP/OOS/MNT/INS
  - P_OOS (SL)
  - Warning
  - P_INS (SL)
  - Warning
  - P_MNT (SL)

- If SL = INS
  - SL = NP/OOS/MNT/INS
  - P_OOS (SL)

- If SL = INS warn
  - else {
    - if SL = OOS
      - discover SL*2
    - init SL*3,
      - SL = INS
  }

- If SL = NE
  - SL = UEQP
  - Add (SL)*
  - Del (SL)*
  - If SL = UEOQP Del (SL)

- If SL = MNT
  - SL = OOS/MNT
  - P_OOS (SL)
  - Warning
  - P_INS (SL)
  - Warning
  - P_MNT (SL)

- If SL = MNT warn
  - else {
    - if SL = OOS
      - discover SL *2
    - init SL*3,
      - SL = MNT
  }

- If SL = OOS
  - SL = NP/UEQP
  - P_OOS (SL)
  - Del (SL)*
  - Add (SL)*
  - P_INS (SL)
  - Warning
  - P_MNT (SL)

- If SL = MNT warn
  - else {
    - if SL = OOS
      - discover SL *2
    - init SL*3,
      - SL = MNT
  }

- If SL = OOS warn
  - if SL = MNT
    - SL = OOS

* Provisioning command
*2 Establish MGCP communication with subscriber loop
*3 Determine capabilities and program terminations

NP = Not provisioned
SL = Subscriber line
Status Command

This section describes how to show the status of subscriber terminations. It is organized as follows:

- Single Subscriber Termination Status
- All Subscriber Terminations Status
- Operating State Token
- Source Token

Single Subscriber Termination Status

This section describes how to check the status of a single subscriber termination.

Step 1

The following example checks the status of a single subscriber termination:

```
status subscriber-termination id=ubr204_1;
```

Reply Example:

```
RESULT -> ADM configure result in success
REASON -> ADM executed successful
ADMIN STATE -> ADMIN_INS
OPER STATE -> Termination is idle
SUBSCRIBER DN -> ubr204_1
FAULT REASON -> No fault reason available
```

Note

Table 17-4 lists the administrative states the system can return.

Table 17-4 Returnable Administrative States

<table>
<thead>
<tr>
<th>State</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMIN-UEQP</td>
<td>Unequipped.</td>
</tr>
<tr>
<td>ADMIN-INS</td>
<td>In Service.</td>
</tr>
<tr>
<td>ADMIN-OOS</td>
<td>Out of Service.</td>
</tr>
<tr>
<td>ADMIN-MAINT</td>
<td>Maintenance Mode.</td>
</tr>
<tr>
<td>ADMIN-OOS-PENDING</td>
<td>Transitioning to Out of Service.</td>
</tr>
<tr>
<td>ADMIN-MAINT-PENDING</td>
<td>Transitioning to Maintenance Mode.</td>
</tr>
</tbody>
</table>

All Subscriber Terminations Status

This section describes how to show the status of all subscriber-terminations on a particular gateway.

Step 1

The following example shows the status of all subscriber-terminations on a particular gateway:

```
status subscriber-termination id=*@ubr235;
```

Reply Example:

Reply Example:
SUBSCRIBER DN -> ubr235_1
ADMIN STATE -> ADMIN_UEQP
OPER STATE -> Termination is unequiped
REASON -> ADM executed successful
RESULT -> ADM configure result in success
FAULT REASON -> No fault reason available

SUBSCRIBER DN -> ubr235_2
ADMIN STATE -> ADMIN_UEQP
OPER STATE -> Termination is unequiped
REASON -> ADM executed successful
RESULT -> ADM configure result in success
FAULT REASON -> No fault reason available

Reply : Success:

Administrative State Token

The Administrative State (admin-state) token returns the administrative state of the subscriber termination. Valid values are:

- **UEQP**—Unequipped; resource is not commissioned. Resource is not registered.
- **OOS**—Termination was manually controlled out of service.
- **INSQ** Termination was manually controlled in service, but operationally may be available or unavailable.
- **OOS-PENDING**—Termination was manually controlled out of service with mode graceful, termination is still involved in a call.
- **MAINT**—Termination was in maintenance mode, can run diagnostic commands.
- **MAINT-PENDING**—Termination was manually controlled to MAINT state, but termination is still involved in call.
- **ALL**—Return all possible states.

The following command example returns only those trunk terminations that are in administrative state OOS (if any), and operating state IDLE (if any):

```
status trunk-termination tgn-id=12; cic=1-1000; admin-state=OOS; oper-state=idle
```

Operating State Token

The Operating State (oper-state) token expands the range of useful information returned by the status subscriber-termination command.

Valid values for the oper-state token are:

- **FA**—Faulty
- **NF**—Not faulty
- **IDLE**—Termination idle
- **ACTIVE**—Termination active
- **DOWN**—Termination down
- **TERM-FA**—Termination fault
TEMP-DOWN—Termination temporarily down
UNREACH—Termination unreachable
INT-MAINT—Termination internal maintenance
UEQP—Termination unequipped
ALL—All states, same as executing command without oper-state token

The following example returns only those subscriber terminations that are FA (if any):

```
status subscriber-termination id=*@ubr235; oper-state=FA;
```

### Source Token

The source token specifies whether to query the Call Agent, or the EMS, for status information. It is an optional token.

Valid values for the source token are:
- EMS (Default)—Query the local EMS database for most current status.
- AGENT—Query the remote Call Agent database for most current status.

The following example returns the current status of a Call Agent:

```
status subscriber-termination id=*@ubr235; source=AGENT;
```

### Control Command

This section describes how to control subscriber terminations on a particular gateway. To control a subscriber termination to the unequipped or equipped state, use the equip or unequip commands in the “Equip Command” section on page 17-13 and the “Unequip Command” section on page 17-13. This section is organized as follows:

- Control a Gateway In Service
- Control All Subscriber Terminations
- Equip Command
- Unequip Command

### Control a Gateway In Service

This section describes how to control a gateway in service.

**Step 1**
The following example controls a gateway into service:

```
control subscriber-termination id=*@c3810_167; mode=forced; target-state=INS;
```

Reply Example:

Reply : Success: CLI change successful

ID -> c3810_167
REQUEST STATE -> ADMIN_INS
RESULT STATE -> ADMIN_INS
FAIL REASON -> ADM found no failure
REASON -> ADM executed successful
Control All Subscriber Terminations

This section describes how to control all subscriber-terminations on a particular gateway.

**Step 1**
The following example controls to MAINT all subscriber-terminations on a particular gateway:

```Shell
control subscriber-termination id=*@ubr235; mode=forced; target-state=MAINT
```

Reply Example:

Reply : Success: CLI change successful

ID -> ubr235
REASON -> ADM executed successful
RESULT -> ADM configure result in success
REQUEST STATE -> ADMIN_MAINT
RESULT STATE -> ADMIN_MAINT
FAIL REASON -> ADM found no failure

CLI>diag subscriber-termination

Reply : Success: Diagnostic Subscriber Menu.

Equip Command

The equip command changes the administrative state of terminations that are in the UEQP state to OOS state. It ignores the terminations in the INS, MAINT, or OOS states.

**Step 1**
Use the following example to equip a subscriber termination:

```Shell
equip subscriber-termination id=97_8@ipclab.cisco.com;
```

Reply Example:

Reply : Success: CLI change successful

ID -> Subscriber ID -> 97_8@ipclab.cisco.com
REASON -> ADM executed successful
RESULT -> ADM configure result in success
FAIL REASON -> ADM found no failure

Unequip Command

The unequip command changes the administrative state of subscriber terminations that are in OOS state into UEQP state. It ignores the terminations in the INS, MAINT, or UEQP states.

**Step 1**
Use the following command to unequip a subscriber termination:

```Shell
unequip subscriber-termination id=97_8@ipclab.cisco.com;
```

Reply Example:

Reply : Success: CLI change successful
Trunk Termination

This section describes the status and control commands for trunk terminations. Either a range (for example, cic=1-24;) or a single value (for example, cic=1;) for the CIC parameter can be specified for the status and control of trunk terminations.

Individual ISDN trunks and trunking groups can be placed into any of three administrative service states: INS, OOS, and MAINT. The relationship between trunk/trunk group state and the TGW state is provided in Table 17-5. For all other trunk types, the trunk state and trunk group state are independent.

Table 17-5 ISDN TGW/TG State Relationships

<table>
<thead>
<tr>
<th>TGW State</th>
<th>Allowed TG States</th>
<th>Allowed Trunk States</th>
</tr>
</thead>
<tbody>
<tr>
<td>INS</td>
<td>• OOS</td>
<td>• UEQP OOS</td>
</tr>
<tr>
<td></td>
<td>• MAINT</td>
<td>• UEQP OSS, MAINT</td>
</tr>
<tr>
<td></td>
<td>• INS</td>
<td>• UEQP OOS, MAINT, INS</td>
</tr>
<tr>
<td>MAINT</td>
<td>• OOS</td>
<td>• UEQP OOS</td>
</tr>
<tr>
<td></td>
<td>• MAINT</td>
<td>• UEQP OSS, MAINT</td>
</tr>
</tbody>
</table>

where:
- TGW—trunking gateway
- TG—trunk group
- OOS—out of service
- MAINT—maintenance
- INS—in service
- UEQP—unequipped

The rules for placing trunks and TG into the OOS, INS, and MAINT states (which depend upon the TGW state) are shown in Figure 17-3.
Figure 17-3  ISDN Administrative and Operational Maintenance States for a Trunking Gateway

- **TGP = OOS**
- **Add (TGP)**
  - **Add (TRK, TGP)**
  - **if TGP = OOS del (TRK)**
  - **TRK = OOS**
- **TGW = OOS**
  - **P_OOS (TGP)**
  - **if TGP = NP**
    - **TGP = OOS**
    - **TRK = NP/OOS**
- **P_INS (TGP)**
  - **if TGP = OOS**
  - **P_OOS (TGP)**
  - **if TGP = NP**
    - **TGP = OOS**
    - **TRK = NP/OOS**
- **P_MNT (TGP)**
  - **if TGP = OOS**
  - **P_OOS (TGP)**
  - **if TGP = NP**
    - **TGP = OOS**
    - **TRK = NP/OOS/MNT/INS**
- **P_INS (TRK, TGP)**
  - **if TGP = OOS**
  - **if TGP = NP**
    - **TGP = OOS**
    - **TRK = NP/OOS/MNT/INS**
- **P_MNT (TRK, TGP)**
  - **if TGP = OOS**
  - **if TGP = NP**
    - **TGP = OOS**
    - **TRK = NP/OOS/MNT/INS**

---

- **TGW = INS**
  - **TGP = NP/OOS/MNT/INS**
  - **TRK = NP/OOS/MNT/INS**
  - **P_INS (TRK, TGP)**
    - **if (TRK, TGP) = INS/MNT**
      - **TGP = OOS**
      - **TRK = OOS**
      - **bearer = OOS**
      - **signaling = OOS**
  - **P_OOS (TRK, TGP)**
    - **if (TRK, TGP) = OOS**
      - **TGP = OOS**
      - **TRK = OOS**
      - **bearer = OOS**
      - **signaling = OOS**
  - **P_MNT (TRK, TGP)**
    - **if (TRK, TGP) = OOS**
      - **TGP = OOS**
      - **TRK = OOS**
      - **bearer = OOS**
      - **signaling = OOS**

---

- **P_OOS = Place out of service**
- **P_INS = Place in service**
- **P_MNT = Place maintenance**
- **NP = Not provisioned**
Status Command

This section describes how to check trunk termination status. This section is organized as follows:

- Trunk Termination Status
- Tokens

Trunk Termination Status

This section describes how to check the status of one trunk termination. This command can be executed for one CIC (for example, cic=1;), a range of CICs (for example, cic=1-12;) or for all CICs (cic=all;).

Step 1

Use the following example to check the status of one trunk termination:

```
status trunk-termination tgn-id=2; cic=8;
```

Reply Example:

```
Reply : Success:
RESULT -> ADM configure result in success
REASON -> ADM executed successful
TGN ID -> 2
CIC -> 8
TERM ADMIN STATE -> ADMIN_INS
TERM OPER STATE -> Termination is idle
TERM REASON -> No fault reason available
TRUNK STATIC STATE -> ACTV
TRUNK DYNAMIC STATE -> TRNS
TRUNK REASON -> NON_FAULTY
```

Note: Table 17-6 lists the administrative states the system can return for the term admin status response.

<table>
<thead>
<tr>
<th>State</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMIN-UNEQP</td>
<td>Unequipped.</td>
</tr>
<tr>
<td>ADMIN-INS</td>
<td>In Service.</td>
</tr>
<tr>
<td>ADMIN-OOS</td>
<td>Out of Service.</td>
</tr>
<tr>
<td>ADMIN-MAINT</td>
<td>Maintenance Mode.</td>
</tr>
<tr>
<td>ADMIN-OOS-PENDING</td>
<td>Transitioning to Out of Service.</td>
</tr>
<tr>
<td>ADMIN-MAINT-PENDING</td>
<td>Transitioning to Maintenance Mode.</td>
</tr>
<tr>
<td>ADMIN-NUL</td>
<td>Resource does not exist.</td>
</tr>
</tbody>
</table>
Tokens

The following optional tokens can be used with the status trunk-termination command. They expand the range of useful information returned. Either all, or none of the tokens can be used, with the exception of the off-normal token, which must be used by itself (without any other tokens).

- Administrative State (admin-state). Valid values are:
  - UEQP—Unequipped; resource is not commissioned. Resource is not registered.
  - OOS—Termination was manually controlled out of service.
  - INS—Termination was manually controlled in service, but operationally may be available or unavailable.
  - OOS-PENDING—Termination was manually controlled out of service with the graceful mode, termination is still involved in a call.
  - MAINT—Termination was in maintenance mode, can run diagnostic commands.
  - MAINT-PENDING—Termination was manually controlled to the MAINT state, but termination is still involved in call.
  - ALL—Return all possible states.

The following command example returns only those trunk terminations that are in administrative state OOS (if any), and operating state IDLE (if any):

```
status trunk-termination tgn-id=12; cic=1-1000; admin-state=OOS; oper-state=idle
```

- Operating State (oper-state). Valid values for the oper-state token are:
  - FA—Includes FAULTY, UNREACH, TEMP-DOWN, and DOWN.
  - FAULTY—The MGCP endpoint returned a permanent error error code.
  - UNREACH—The MGCP endpoint was declared as not reachable. This indicates gateway connectivity problems.
  - TEMP-DOWN—The MGCP endpoint is temporarily down.
  - DOWN—MGCP endpoint is down because GW termination has sent an RSIP-down message.
  - NF—Includes INT-MAINT, IDLE, BUSY, and ACTIVE.
  - INT-MAINT—Internal error recovery is in progress.
  - IDLE—Termination is not involved in a call, but is available.
  - BUSY—Termination is involved in transient call.
  - ACTIVE—Termination is involved in stable call.
  - UEQP—Termination is not equipped.
  - ALL—Returns all possible operational states.

The following command example returns only those trunk terminations that are FA (if any):

```
status trunk-termination tgn-id=12; cic=ALL; oper-state=FA;
```

- Static State (static-state). Valid values for the static-state token are:
  - UEQP—Unequipped resource is not commissioned. Resource is not registered.
  - LBLK—Termination is locally blocked: either manually taken OOS/MAINT (block reason can be MANUAL-OOS, MAINT-OOS), or automatically went out of service.
  - RBLK—Termination is remotely blocked (blocked by remote side).
Trunk Termination

- ACTV—Available.
- All—Returns all possible static states.

The following command example returns only those terminations that are locally blocked (if any):

```
status trunk-termination tgn-id=101; cic=1-24; static-state=lblk;
```

- **Dynamic State** (dynamic-state). Valid values for the dynamic-state token are:
  - IBSY—Trunk-termination is involved in an incoming active call.
  - OBSY—Trunk-termination is involved in an outgoing active call.
  - TRNS—Transient maintenance state (sent maintenance signaling message and waiting for response).
  - IDLE—Termination is not involved in a call.
  - IBSY-TRNS—Termination is involved in an incoming transient call.
  - OBSY-TRNS—Termination is involved in an outgoing transient call.
  - ALL—All possible dynamic states.

The following command example returns only those terminations that are idle (if any):

```
status trunk-termination tgn-id=101; cic=1-24; dynamic-state=idle;
```

- **Off-normal State** (off-normal)
  - Yes—Return all terminations in off-normal state.
  - No—Return all terminations in normal state.

The following command example returns only those terminations in an off-normal state (if any).

```
status trunk-termination tgn-id=101; cic=1-24; off-normal=yes;
```

A termination is in an off-normal state when it is not in one of the state combinations shown in Table 17-7.

- **Source** (source)—Specifies whether to query the Call Agent or the Element Management System (EMS) for status information. It is an optional token.
  - EMS (Default)—Query the local EMS database for most current status.
  - AGENT—Query the remote Call Agent database for most current status.

The following command example returns the current status of the Call Agent:

```
status trunk-termination tgn-id=101; cic=1-24; source=AGENT;
```

### Table 17-7 Valid Normal Trunk Termination States

<table>
<thead>
<tr>
<th>State/Token</th>
<th>ADMIN-STATE</th>
<th>OPER-STATE</th>
<th>STATIC-STATE</th>
<th>DYNAMIC-STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNEQP</td>
<td>UNEQP</td>
<td>ANY</td>
<td>UNEQP</td>
<td>IDLE</td>
</tr>
<tr>
<td>MANUALLY OOS</td>
<td>OOS</td>
<td>ANY</td>
<td>LBLK</td>
<td>IDLE</td>
</tr>
<tr>
<td>MANUALLY MAIN</td>
<td>MAINT</td>
<td>IDLE</td>
<td>LBLK</td>
<td>IDLE</td>
</tr>
<tr>
<td>IDLE</td>
<td>INS</td>
<td>IDLE</td>
<td>ACTV</td>
<td>IDLE</td>
</tr>
<tr>
<td>ACTIVE INCOMING</td>
<td>INS</td>
<td>IDLE</td>
<td>ACTV</td>
<td>IDLE</td>
</tr>
<tr>
<td>ACTIVE OUTGOING</td>
<td>INS</td>
<td>ACTIVE</td>
<td>ACTV</td>
<td>OBSY</td>
</tr>
</tbody>
</table>
This section describes how to control trunk terminations. The section is organized as follows:

- **Control One Trunk Termination**
- **Control All Trunk Terminations**

### Control One Trunk Termination

This section describes how to control a trunk termination.

**Step 1**

Use the following example to control one trunk termination into OOS:

```
control trunk-termination tgn-id=22; cic=1; target-state=OOS; mode=forced;
```

Reply Example:

```
Reply : Success: CLI change successful

TGN ID -> 22
REASON -> ADM executed successful
RESULT -> ADM configure result in success
CIC START -> 1
CIC END -> 1
FAIL REASON -> ADM found no failure
REQUEST STATE -> ADMIN_OOS
RESULT STATE -> ADMIN_OOS
```

### Control All Trunk Terminations

This section describes how to control all trunk terminations for a group of circuit identification codes (CICs).

**Step 1**

Use the following example to control all trunk terminations for a particular CIC group to OOS:

```
control trunk-termination tgn-id=17; cic=1-23; target-state=oos; mode=forced;
```

Reply Example:

```
Reply: Request was successful.

TGN ID -> 17
REASON -> ADM executed successful
RESULT -> ADM configure result in success
CIC START -> 1
CIC END -> 24
FAIL REASON -> ADM found no failure
```

### Table 17-7 Valid Normal Trunk Termination States (continued)

<table>
<thead>
<tr>
<th>State/Token</th>
<th>ADMIN-STATE</th>
<th>OPER-STATE</th>
<th>STATIC-STATE</th>
<th>DYNAMIC-STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRANSIENT INCOMING</td>
<td>INS</td>
<td>ACTIVE</td>
<td>ACTV</td>
<td>IBY-TRNS</td>
</tr>
<tr>
<td>TRANSIENT OUTGOING</td>
<td>INS</td>
<td>BUSY</td>
<td>ACTV</td>
<td>OBSY-TRNS</td>
</tr>
</tbody>
</table>
REQUEST STATE -> ADMIN_OOS
RESULT STATE -> ADMIN_OOS

Reset Command

The reset command clears all manual and blocked states as well as any active/transient calls on a trunk termination, with the exception of SS7 trunk terminations. It brings a trunk into INS mode. This section is organized as follows:

- Reset a Single CIC
- Reset a Range of CICs
- Reset All CICs

Reset a Single CIC

This section describes how to reset a single CIC.

Step 1

The following example resets a single CIC on a specific trunk:

```
reset trunk-termination tgn-id=22; cic=1
```

Reply Example:

```
Reply : Success:
   TGN ID   -> 22
   REASON   -> ADM executed successful
   RESULT   -> ADM configure result in success
   CIC START -> 1
   CIC END   -> 1
   FAIL REASON -> ADM found no failure
```

Reset a Range of CICs

This section describes how to reset a range of CICs.

Step 1

The following example resets a range of CICs on a specific trunk:

```
reset trunk-termination tgn-id=13; cic=1-6;
```

Reply Example:

```
TGN ID   -> 13
REASON   -> ADM executed successful
RESULT   -> ADM configure result in success
CIC START -> 1
CIC END   -> 6
FAIL REASON -> ADM found no failure
```
Chapter 17      Maintenance and Diagnostics: External Resources

Trunk Termination

Reset All CICs

This section describes how to reset all CICs.

Step 1

The following example resets all CICs on a specific trunk:

 resets trunk-termination tgn-id=13; cic=all;

Reply Example:

 TGN ID -> 13
 REASON -> ADM executed successful
 RESULT -> ADM configure result in success
 CIC START -> 1
 CIC END -> 24
 FAIL REASON -> ADM found no failure

Equip Command

The equip command changes the administrative state of terminations that are in the UEQP state to the OOS state. It ignores the terminations in the INS, MAINT, or OOS states.

Note

[For an ISDN trunk, a trunk termination can be equipped using this command. It can also be equipped using the control trunk-grp command—this command puts all trunks in the specified trunk group into the specified target state. However, for all other trunk types, the trunk termination must be equipped using the equip command. Then control the termination into other states using the control command.]

- A termination must be in the UEQP state before deleting it.
- UEQP is not a target-state for the control command. When using the control command, any trunk termination in an UEQP state will not be affected. For example, if there are 24 CICs in a trunk group, and the initial states of the CICs are:

  CICs 1-10 in OOS state, 11-15 in UEQP state, and 16-24 in MAINT state.

1. If a control command is used with target-state=ins, the final states of all the CICs are:
   CICs 1-10 in INS state, 11-15 in UEQP state, and 16-24 in INS state.
2. If an equip command is applied to the CICs in the initial states, the final states of all the CICs are:
   CICs 1-10 in OOS state, 11-15 in OOS state, and 16-24 in MAINT state.
3. If an unequip command is applied to the CICs in the initial states, the final states of the CICs are:
   CICs 1-10 in UEQP state, 11-15 in UEQP state, and 16-24 in MAINT state.

Step 1

Use the following example to equip a trunk termination:

 equp trunk-termination tgn-id=13; cic=all;

Reply Example:

 Reply : Success: CLI change successful

 TGN ID -> 13
 REASON -> ADM executed successful
 RESULT -> ADM configure result in success
 CIC START -> 1
 CIC END -> 24
Unequip Command

The unequip command changes the administrative state of terminations that are in the OOS state into the UEQP state. It ignores the terminations in the INS, MAINT, or UEQP states.

Step 1

Use the following example to unequip terminations:

```
unequip trunk-termination tgn-id=13; cic=all;
```

Reply Example:

```
Reply : Success: CLI change successful
TGN ID -> 13
REASON -> ADM executed successful
RESULT -> ADM configure result in success
CIC START -> 1
CIC END -> 24
```

Diagnostic Tests

This section describes diagnostic tests that can be performed on media gateways, subscriber terminations, and trunk terminations. All media gateways, subscriber and trunk terminations must be in the MAINT state for testing.

Media Gateway Tests

This section describes the tests that can be performed on media gateways. A gateway must be in the MAINT state.

Step 1

Force the media gateway into MAINT state:

```
control mgw id=c2421.65; mode=forced; target-state=maint;
```

Step 2

Display the Test Menu.

```
diag mgw
```

Reply Example:

```
Reply: Diagnostic MGW Menu.
===
(1) MGW Network Connectivity Test
(2) MGW MGCP Connectivity Test
(3) ALL
```

Note

Test #1 tests if there is a path to the device (ping).
Test #2 tests if MGCP has access to the device.
Test #3 performs tests 1 and 2.
**Chapter 17      Maintenance and Diagnostics: External Resources**

**Diagnostic Tests**

**Step 3**
To perform a specific test, use the following examples as a guide.

```plaintext
diag mgw id=ubr-03; test=1;
diag mgw id=ubr-03; test=2;
diag mgw id=ubr-03; test=3;
```

---

**Subscriber Termination Tests**

This section describes the tests that can be performed on subscriber terminations. All terminations must be in the MAINT state.

**Step 1**
Force the subscriber termination into MAINT state:

```plaintext
control subscriber-termination id=sub2-ctx2; mode=forced; target-state=maint;
```

**Step 2**
Display the Test Menu.

```plaintext
diag subscriber-termination;
```

Reply Example:

```
Reply: Diagnostic Subscriber Menu.
===
(1) Subscriber MGCP Connectivity Test
(2) Subscriber Termination Connection Test
(3) Subscriber Termination Ring Test
(4) ALL
```

**Note**
Test #1 tests if MGCP has access to the termination.
Test #2 tests if there is a path to the device (ping).
Test #3 tests if the subscriber can be rung. The Ring parameter must be specified in seconds for this test. The default is 5 seconds.
Test #4 performs tests 1 through 3.

**Step 3**
To perform a specific test, use the following examples as a guide.

```plaintext
diag subscriber-termination id=sub2-ctx2; test=1;
diag subscriber-termination id=sub-ubr3-1@cisco.com; test=2;
diag subscriber-termination id=sub-ubr3-1@cisco.com; test=3; ring-duration=10;
diag subscriber-termination id=sub-ubr3-1@cisco.com; test=3; ring-duration=10;
```

**Note**
Ring-duration values are 0–999 (Default = 5). Maximum ring time is 30 seconds regardless of whether the duration is set higher than or equal to 31.
Trunk Termination Tests

This section describes diagnostic tests that can be performed on trunk terminations. All terminations must be in the MAINT state for testing. Trunk termination tests are done by trunk type.

SS7 Trunk Termination Tests

This section describes the tests that can be performed on SS7 trunk terminations.

---

**Step 1**

Force the SS7 trunk termination into MAINT state:

```
control ss7-trunk-termination tgn-id=103; mode=forced; target-state=maint;
```

**Note**

Set COT, CVM, and CQM on the terminating gateway or switch to perform these tests. Otherwise, the test or tests will fail.

**Step 2**

Display the Test Menu.

```
diag ss7-trunk-termination
```

Reply Example:

```
Reply: Diagnostic SS7 Trunk Group Menu.

(1) SS7 MGCP Connectivity Test
(2) SS7 Termination Connection Test
(3) SS7 COT Test
(4) SS7 CQM Test
(5) SS7 CVT Test
(6) ALL
```

**Note**

Test #1 tests if MGCP has access to the SS7 trunk termination.
Test #2 tests if there is a path to the device (ping).
Test #3 tests the integrity of the SS7 Bearer Path.
Test #4 queries the SS7 circuit (or group of circuits) status. A range of CICs can be specified (to a maximum of 24). Both remote and local trunk states are displayed in the results.
Test #5 tests to ensure that each end of the circuit has sufficient and consistent information for using the circuit in call connections. CLLI names are included.
Test #6 performs tests 1 through 5.

**Step 3**

To perform a specific test, use the following examples as a guide:

```
diag ss7-trunk-termination tgn-id=103; cic=13; test=1;
diag ss7-trunk-termination tgn-id=103; cic=13; test=2;
diag ss7-trunk-termination tgn-id=103; cic=14; test=3;
diag ss7-trunk-termination tgn-id=2; cic=1-24; test=4;
diag ss7-trunk-termination tgn-id=2; cic=1; test=5;
```
ISDN Trunk Termination Tests

This section describes the tests that can be performed on ISDN trunk terminations.

**Step 1** Force the ISDN trunk termination into MAINT state:
```
control isdn-trunk-termination tgn-id=17; mode=forced; target-state=maint;
```

**Step 2** Display the Test Menu.
```
diag isdn-trunk-termination
```
Reply Example:
```
Reply: Diagnostic ISDN Trunk Group Menu.
===
(1) ISDN MGCP Connectivity Test
(2) ISDN Termination Connection Test
(3) ALL
```

**Note**
Test #1 tests if MGCP has access to the ISDN termination.
Test #2 tests if there is a path to the device (ping).
Test #3 performs tests 1 and 2.

**Step 3**
To perform a specific test, use the following examples as a guide:
```
diag isdn-trunk-termination test=1; tgn-id=17; cic=1;
diag isdn-trunk-termination test=2; tgn-id=17; cic=1;
```

CAS Trunk Termination Tests

This section describes the tests that can be performed on CAS trunk terminations.

**Step 1** Force the CAS trunk termination into MAINT state:
```
control cas-trunk-termination tgn-id=64; mode=forced; target-state=maint;
```

**Step 2** Display the Test Menu.
```
diag cas-trunk-termination
```
Reply Example:
```
Reply: Diagnostic CAS Trunk Group Menu.
===
(1) CAS MGCP Connectivity Test
(2) CAS Termination Connection Test
(3) ALL
```

**Note**
Test #1 tests if MGCP has access to the CAS termination.
Test #2 tests if there is a path to the device (ping).
Test #3 performs tests 1 and 2.

**Step 3**
To perform a specific test, use the following examples as a guide:
```
diag cas-trunk-termination tgn-id=64; cic=1; test=1;
```
Command Responses

This section describes success and failure responses to commands, as well as values for the term-reason and trunk-reason responses.

Generic Responses to Status or Control Command Failures

These generic status and control commands apply to all MGWs, subscribers, trunks, and trunk groups. If a command fails, it can return one of the following generic failure reasons, as well as ones specific to the command (shown in following sections).

- Subscriber, media gateway, trunk group or trunk database was not found in shared memory.
- Component is already in the requested state.
• Graceful mode only. Appears when a command is executed and operation is INS going OSS or INS going MAINT.
• A required resource is not available.
  If the MGW for a subscriber is down, the subscriber cannot be added.
  For ISDN
  - A trunk cannot be added unless both the MGW and trunk group are available.
  - A trunk group cannot be added unless the MGW is available, and vice versa.
  For SS7, CAS, Announcement
  - A trunk cannot be added unless both the MGW and trunk group are available.
  - A trunk group does not require the MGW to be available, and vice versa.
• An associated resource of the database cannot be found.
• An assigned resource is not valid (supported). For example: A subscriber is assigned to a PBX and the PBX is not supported.

**Generic Success and Failure Responses**

The following message is returned upon the success of a command:
• Configuration Command Executed.

One of the following messages can be returned upon the failure of a command:
• ADM found no failure.
• ADM MGW(s) cannot be found.
• ADM subscriber(s) cannot be found.
• ADM trunk group(s) cannot be found.
• ADM trunk(s) cannot be found.
• ADM no termination(s) found in MGW.
• ADM no trunk group(s) found in trunking gateway.
• ADM no trunk(s) found in trunk group.
• ADM fail while in termination table.
• ADM fail while in trunk group table.
• ADM fail while in trunk table.
• ADM fail while looking to find trunk index.
• ADM fail while getting MGW administration state.
• ADM fail while getting trunk group administration state.
• ADM fail while looking for MGW index.
• ADM administration state invalid.
• ADM failed to allocate IPC message(s).
• ADM failed to dispatch IPC message(s).
• ADM operational state invalid.
Command Responses

- ADM MGW(s) state change and pending.
- ADM subscriber(s) state change and pending.
- ADM trunk group(s) state change and pending.
- ADM trunk(s) state change and pending.
- ADM found subscriber category invalid.
- ADM found trunk group type invalid.
- ADM found trunk group state invalid.
- ADM found MGW admin state not ready.
- ADM found trunk group admin state not ready.
- ADM entity in desired state.
- ADM not allow trunk to reset.
- ADM not allow subscriber to reset.
- ADM change to out-of-service state required.
- ADM change to request graceful mode error.
- ADM found entity unequipped in initial state.
- ADM operation not allowed because D Channel(s) is down.
- The H.323 Gateway was not found in DBM.
- ADM found unknown failure reason(s).

System Error Response

[The following error message applies to system processes, not just specific databases and their commands:

- Shared memory conflict between processes]

Termination Reason Responses

The following statements can be returned for the termination reason (term-reason) response for subscriber termination and trunk termination commands:

- The media gateway is down.
- The media gateway is unreachable.
- The media gateway is in a faulty state.
- The media gateway is transitioning to another state.
- The transaction could not be executed due to a transient error.
- The transaction could not be executed because the endpoint is unknown.
- The transaction could not be executed because the endpoint is not ready.
- The transaction could not be executed, endpoint doesn't have enough resources available.
- The transaction could not be executed because a protocol error was detected.
- The transaction could not be executed because the command contained an unrecognized extension.
• The transaction could not be executed because the gateway is not equipped to detect one of the requested events.
• The transaction could not be executed because the gateway is not equipped to generate one of the requested signals.
• The transaction could not be executed because the gateway cannot send the specified announcement.
• Invalid conn identifier.
• Invalid call ID.
• Unsupported mode or invalid mode.
• Unsupported or unknown package.
• Endpoint does not have a digit map.
• The transaction could not be executed because the endpoint is restarting.
• Endpoint redirected to another Call Agent.
• No such event or signal.
• Unknown action or illegal combination of actions.
• Internal consistency in local connection options.
• Unknown extensions in local connection options.
• Insufficient bandwidth.
• Missing remote connection descriptor.
• Incompatible protocol version.
• Internal hardware failure.
• CAS signaling protocol error.
• Failure of a group of trunks.
• Unsupported values on local connection options.
• Response too big.
• Endpoint malfunctioning.
• Loss of lower connectivity.
• Endpoint taken out of service.
• No fault reason available.

**Trunk Reason Responses**

The following statements can be returned for the trunk reason (trunk-reason) response. One or more statements can be returned, depending upon the operating conditions of the Call Agent.

• NON-FAULTY—Not blocked, available for service.
• MAINT-OOS—trunk-termination is manually controlled OOS.
• MAINT-BUSY—trunk-termination is in maintenance state; controlled to MAINT.
• TERM-FAULT—Bearer termination is in faulty condition.
• SIGNALLING-FAULT—Signaling link (for example, SS7 link, or ISDN D-channel) is faulty.
• MAINT-BLOCK—trunk-termination is manually controlled OOS (controlled mode=GRACE).
• HARDWARE-BLOCK—trunk-termination is manually controlled OOS (controlled mode=FORCED).
• OUTGOING_RESTRICTED—the outgoing call is not allowed
• DPC_INACCESSIBLE—the DPC is not accessible.

The following responses are returned as of Release 3.5.3:
• ACL_CONGESTION_LEVEL_1—Automatic Congestion Level (ACL) congestion is at level 1.
• ACL_CONGESTION_LEVEL_2—ACL congestion is at level 2.
• ACL_CONGESTION_LEVEL_3—ACL congestion is at level 2.
• TFC_CONGESTION_LEVEL_1—Transfer Controlled (TFC) congestion is at level 1.
• TFC_CONGESTION_LEVEL_2—TFC congestion is at level 2.
• TFC_CONGESTION_LEVEL_3—TFC congestion is at level 3.

Fault Reason Responses (Release 3.3)

The following statements can be returned for the fault reason (fault-reason) response for a subscriber termination command. One or more statements can be returned, depending upon the operating conditions of the Call Agent.
• The media gateway is down.
• The media gateway is unreachable.
• The media gateway is in a faulty state.
• The media gateway is transitioning to another state.
• The transaction could not be executed, due to a transient error.
• The transaction could not be executed because the endpoint is unknown.
• The transaction could not be executed because the endpoint is not ready.
• The transaction could not be executed, endpoint doesn't have enough resources available.
• The transaction could not be executed because a protocol error was detected.
• The transaction could not be executed because the command contained an unrecognized extension.
• The transaction could not be executed because the gateway is not equipped to detect one of the requested events.
• The transaction could not be executed because the gateway is not equipped to generate one of the requested signals.
• The transaction could not be executed because the gateway cannot send the specified announcement.
• Invalid conn identifier.
• Invalid call ID.
• Unsupported mode or invalid mode.
• Unsupported or unknown package.
• Endpoint does not have a digit map.
• The transaction could not be executed because the endpoint is restarting.
• Endpoint redirected to another Call Agent.
• No such event or signal.
• Unknown action or illegal combination of actions.
• Internal consistency in local connection options.
• Unknown extensions in local connection options.
• Insufficient bandwidth.
• Missing remote connection descriptor.
• Incompatible protocol version.
• Internal hardware failure.
• CAS signaling protocol error.
• Failure of a group of trunks.
• Unsupported values on local connection options.
• Response too big.
• Endpoint malfunctioning.
• Loss of lower connectivity.
• Endpoint taken out of service.
• No fault reason available.
Managing Billing Interface and Billing Records

The billing subsystem on the Element Management System (EMS) gathers all billing-related call events from call processing, formats them into a standard format, and transmits them to an external collection device. The interface to the billing mediation device can vary from carrier to carrier, thus this subsystem supports a flexible profiling system.

The billing subsystem includes the following functions:

- Provides FTP transfer of call data records to a remote billing server
- Supports batch record transmission via FTP
- Issues events and alarms as appropriate, including potential billing data overwrites
- Saves up to 48 hours of billing data in persistent store
- Supports user-provisionable billing subsystem tokens
- Supports on-demand call detail block (CDB) queries based on ranges of timestamps, ranges of sequence numbers, a calling number, a called number, or last record written

Refer to the Cisco BTS 10200 Softswitch Release 3.5 Billing Interface Guide for detailed information on the billing subsystem.

Record Retention Mechanisms in the EMS

The system can hold up to 10 million records in a circular file for 48 hours, depending upon the number of calls per hour. Once this number of records is reached, the next entry rolls over to the first record in the database and starts overwriting from this record onward.

The following sample calculation is determining the number of records at 100 calls per second that can be stored in 48 hours:

100 calls/second in busy hour yields an average daily mean of 45 calls/second X 60 seconds/minute X 60 minutes/hour X 48 hours = 7,776,600 records.

Billing Alarm Tracking Mechanisms

The billing manager process in the EMS tracks the total number of records the billing database can store, the number of unacknowledged records, and the current percentage of the database that is occupied by unacknowledged records. This information is then compared against the threshold levels set in the
billing alarm database. If the current amount of billing data exceeds thresholds in the database, then the billing manager issues alarms. The billing manager resets the alarms as the storage levels drop below the thresholds.

Call Detail Block Correlation and Format

CDBs are produced from the current information sent from the billing generator in the Call Agent (CA) to the billing manager in the Bulk Data Management System (BDMS). Each of the billing event messages (BEM) that are portions of a call in progress are stored in a staging area in the billing generator, waiting for call completion. Once the complete call content is present, the CDB is constructed from the individual BEMs and sent to the billing manager in the BDMS.

Northbound Billing Data Transport

Billing data (batch files containing the CDBs) is transported using FTP to the customer’s Operations Support System (OSS) network. Figure 18-1 shows a typical northbound billing data transport flow. Contact Cisco TAC for billing questions for your specific softswitch system.
Figure 18-1 Billing Database Redundancy and Scalability Configuration

- **Remote accounting office**
  - FTP connection
  - A1000
  - EMS-B Batch file staging area
  - Local disk
  - EMS tracking area
  - Outbound BEMs
  - Local disk

- **MS-A**
  - Batch file staging area
  - Local disk
  - EMS tracking area
  - Outbound BEMs
  - Local disk

- **EMS-B**
  - Batch file staging area
  - Local disk
  - EMS tracking area
  - Outbound BEMs
  - Local disk

- **A-A**
  - Correlation staging area
  - TCP connection

- **CA-B**
  - Correlation staging area
  - TCP connection
Traffic Measurements

This chapter describes how to report traffic measurements on the Cisco BTS 10200 Softswitch.

Traffic Management Subsystem

The Traffic Management Subsystem provides the following functions:

- Collects all statistics in 15, 30, and 60 minute intervals
- Clears counters after each interval without loss of ongoing counts
- Saves 48 hours of statistical data in increments of 15, 30, and 60 minutes in persistent store
- Provides display of summary report of past 48-hour period
- Provides for on-demand report queries keyed by collection interval
- Issues events as appropriate

Filtering Traffic Measurements

Use the following commands to specify which types of measurements are to be stored in the system:

```
show measurement-prov type=<type>;
```

Valid values for <type> are:

- ISDN
- CALLP
- MGA
- SIM
- POTS-FS
- AIN-FS
- ISUP
- SIA
- BILLING
- SNMP
- TG-USG
Retrieving Traffic Measurement Summaries

Use the following commands to retrieve specific types of measurement summaries from the data that are stored in the system:

- `report measurement-ain-fs-summary start-time=<start time>; end-time=<end time>; feature-server-id=<FS ID>;`
- `report measurement-billing-summary start-time=<start time>; end-time=<end time>; call-agent-id=<CA ID>;`
- `report measurement-callp-summary start-time=<start time>; end-time=<end time>; call-agent-id=<CA ID>;`
- `report measurement-isdn-summary start-time=<start time>; end-time=<end time>; call-agent-id=<CA ID>;`
- `report measurement-isup-summary start-time=<start time>; end-time=<end time>; call-agent-id=<CA ID>;`
- `report measurement-mga-summary start-time=<start time>; end-time=<end time>; mgw-id=<MGW ID>;`
- `report measurement-pots-fs-summary start-time=<start time>; end-time=<end time>; feature-server-id=<FS ID>;`
- `report measurement-sia-summary start-time=<start time>; end-time=<end time>; call-agent-id=<CA ID>;`
- `report measurement-sim-summary start-time=<start time>; end-time=<end time>; call-agent-id=<CA ID>;`
- `report measurement-snmp-summary start-time=<start time>; end-time=<end time>;`
- `report measurement-tg-usage-summary start-time=<start time>; end-time=<end time>; tg-type=<TG type>; call-agent-id=<CA ID>; where <TG type>=CAS, ANNC, ISDN, SS7, or SOFTSW`
- `report measurement-anm-summary start-time=<start time>; end-time=<end time>; call-agent-id=<CA ID>;`
- `report measurement-h323-summary start-time=<start time>; end-time=<end time>;`

Note: These commands are not case sensitive. Refer to the Cisco BTS 10200 Command Line Interface Reference Guide for additional details on these commands.
Note
<time> must be entered in the format time=yyyy-mm-dd hh:mm:ss;

<FS ID> is the ID of the selected Feature Server in the feature-server table

<CA ID> is the ID of the selected Call Agent in the call-agent table

<MGW ID> is the ID of the selected media gateway in the mgw table

MGA=media gateway adapter
SIA=SIP-T adapter, SIM=service interaction module

Note
The <time> value can be any time during the 15-, 30-, and 60-minute interval for which the summary is requested. Each 30-minute collection interval starts on the hour or half-hour. If busy-hour data is needed, measurement summaries can be taken from 10:00 to 10:30 a.m. and from 10:30 to 11:00 a.m. Monday through Friday, or at the provider’s own busy hour.

Format of Traffic Measurement Summaries

A traffic measurement summary lists the counters of the type requested in the report command, followed by the count. An example of a report is shown below.

>================================== Start Traffic Report ===============

ANM_TPM_CKT_UNAVAIL  25
ANM_TPM_CALL_REJECTED  3
ANM_TPM_ADDR_INCOMPLETE  11
ANM_TPM_FAC_REJECTED  0
ANM_TPM_PRE_0_1_ABSENT  8
ANM_TPM_PRE_0_1_PRESENT  21
ANM_TPM_HNPA_ABSENT  30
ANM_TPM_NO_ROUTE_DEST  17
ANM_TPM_UNALLOCATED_NUM  0
ANM_TPM_NUM_CHANGED  3
ANM_TPM_DEST_OUTOFORDER  8
ANM_TPM_TEMP_DISCONNECT  15
ANM_TPM_FEAT_NOT_SUBS  2
ANM_TPM_AUTHCODE_INVALID  23
List of Traffic Measurements (Counters)

The tables in this section list the various types of measurements (counters) that are collected by the Cisco BTS 10200 Softswitch. The measurements are grouped into logical categories for easy identification.

It is useful to monitor the measurements that are most important to your operation. Some of the measurements are particularly useful in alerting you to potential problems in the system. In some cases a rapid buildup of counts might indicate a problem such as congestion or processing failures, and so on. In the tables below, an asterisk (*) identifies measurements for which a rapid increase in counts indicates a potential problem.

In addition, some potential network problems can be noticed by looking at specific pairs of measurements that should normally be equal. For example:

- SIP_TOTAL_INCOMING_MSG and SIP_TOTAL_SUCCESS_INCOMING_MSG
  In this case, the total number of successful incoming messages should be about equal to the total number of incoming messages. Any difference between the two counts, especially a rapidly growing difference, might indicate a problem.
- SNMP_SET_TX and SNMP_SET_RX
  In this case, the total number of received SNMP SET commands should be about equal to the total number of transmitted SNMP SET commands. Differences between the two measurements might indicate a potential problem.

The greater the difference between two measurements (when those two measurements should be equal), the more likely it is that there can be a problem in the system.

Resources and Definitions

The following reference materials can assist you in interpreting and using these tables:

- For information on subscriber features, refer to the “Subscriber Features” chapter in the Cisco BTS 10200 Softswitch System Description document.
- For a list of acronyms, see the “Acronyms” appendix in the Cisco BTS 10200 Softswitch System Description document.
## CA and POTS FS Measurement Counters for SIP Messages and Subscriber Features

Table 19-1 describes the Call Agent (CA) and plain old telephone service (POTS) Feature Server measurement counters for Session Initiation Protocol (SIP) messages and subscriber features.

**Table 19-1  CA and POTS FS Measurement Counters for SIP Messages and Subscriber Features**

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_TOTAL_INCOMING_MSG</td>
<td>The total number of SIP messages attempted to be received by the reporting Call Agent or Feature Server (both requests and responses).</td>
</tr>
<tr>
<td>SIP_TOTAL_SUCCESS_INCOMING_MSG</td>
<td>The total number of SIP messages received successfully by the reporting Call Agent or Feature Server (both requests and responses).</td>
</tr>
<tr>
<td>SIP_TOTAL_OUTGOING_MSG</td>
<td>The total number of SIP messages attempted to be transmitted by the reporting Call Agent or Feature Server (both requests and responses).</td>
</tr>
<tr>
<td>SIP_TOTAL_SUCCESS_OUTGOING_MSG</td>
<td>The total number of SIP messages transmitted successfully by the reporting Call Agent or Feature Server (both requests and responses).</td>
</tr>
<tr>
<td>SIP_REQ_RETRAN_RCVD</td>
<td>The total number of SIP request retransmission messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_REQ_RETRAN_SENT</td>
<td>The total number of SIP request retransmission messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_RSP_RETRAN_RCVD</td>
<td>The total number of SIP response retransmission messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_RSP_RETRAN_SENT</td>
<td>The total number of SIP response retransmission messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_T1_TIMER_EXPIRED</td>
<td>*The total number of T1 Timer expirations that occurred during the current collection interval on the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_T2_TIMER_REACHED</td>
<td>*The total number of T2 Timer expirations that occurred during the current collection interval on the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_INVITE_RECEIVED</td>
<td>The total number of INVITE messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_INVITE_SENT</td>
<td>The total number of INVITE messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
</tbody>
</table>
### Table 19-1 CA and POTS FS Measurement Counters for SIP Messages and Subscriber Features (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_CANCEL_RECEIVED</td>
<td>The total number of CANCEL messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_CANCEL_SENT</td>
<td>The total number of CANCEL messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_BYE_RECEIVED</td>
<td>The total number of BYE messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_BYE_SENT</td>
<td>The total number of BYE messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_ACK_RECEIVED</td>
<td>The total number of ACK messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_ACK_SENT</td>
<td>The total number of ACK messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_OPTIONS_RECEIVED</td>
<td>The total number of OPTION messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_OPTIONS_SENT</td>
<td>The total number of OPTION messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_REGISTER_RECEIVED</td>
<td>The total number of REGISTER messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_REGISTER_SENT</td>
<td>The total number of REGISTER messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_INFO_RECEIVED</td>
<td>The total number of INFO messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_INFO_SENT</td>
<td>The total number of INFO messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_NOTIFY_RECEIVED</td>
<td>The total number of NOTIFY messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_NOTIFY_SENT</td>
<td>The total number of NOTIFY messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_100_RECEIVED</td>
<td>The total number of 100 (trying) messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_100_SENT</td>
<td>The total number of 100 (trying) messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
</tbody>
</table>
### List of Traffic Measurements (Counters)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_18x_RECEIVED</td>
<td>The total number of 18x (informational) messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_18x_SENT</td>
<td>The total number of 18x (informational) messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_200_RECEIVED</td>
<td>The total number of 200 (success) messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_200_SENT</td>
<td>The total number of 200 (success) messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_3xx_RECEIVED</td>
<td>The total number of 3xx (redirection) messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_3xx_SENT</td>
<td>The total number of 3xx (redirection) messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_4xx_RECEIVED</td>
<td>*The total number of 4xx (request failures) messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_4xx_SENT</td>
<td>*The total number of 4xx (request failures) messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_5xx_RECEIVED</td>
<td>*The total number of 5xx (server failures) messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_5xx_SENT</td>
<td>*The total number of 5xx (server failures) messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_6xx_RECEIVED</td>
<td>*The total number of 6xx (global failures) messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_6xx_SENT</td>
<td>*The total number of 6xx (global failures) messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_7xx_RECEIVED</td>
<td>The total number of 7xx (reserved) messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_7xx_SENT</td>
<td>The total number of 7xx (reserved) messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
</tbody>
</table>
### Table 19-1 CA and POTS FS Measurement Counters for SIP Messages and Subscriber Features (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_PROV_RSP_RETRAN_RCVD</td>
<td>The number of SIP provisioning response retransmission messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_PROV_RSP_RETRAN_SENT</td>
<td>The number of SIP provisioning response retransmission messages sent by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_PRACK_RECEIVED</td>
<td>The number of SIP PRACK messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_PRACK_SENT</td>
<td>The number of SIP PRACK messages sent by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_SUBSCRIBE_RECEIVED</td>
<td>The number of SIP SUBSCRIBE messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_SUBSCRIBE_SENT</td>
<td>The number of SIP SUBSCRIBE messages sent by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_REFER_RECEIVED</td>
<td>The number of SIP REFER messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_REFER_SENT</td>
<td>The number of SIP REFER messages sent by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_REFER_REPLACES_RECEIVED</td>
<td>The number of SIP REFER REPLACES messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_INVITE_REPLACES_SENT</td>
<td>The number of SIP INVITE REPLACES messages sent by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_REL100_RECEIVED</td>
<td>The number of REL100 class (TRYING) messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_REL100_SENT</td>
<td>The number of REL100 class (TRYING) messages sent by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_UNSUPPORTED_RECEIVED</td>
<td>The number of unsupported SIP messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>POTS_CFU_ACTIVATION_ATTEMPTS</td>
<td>The number of Call Forward Unconditional activation attempts on the reporting POTS Feature Server.</td>
</tr>
</tbody>
</table>
Table 19-1  CA and POTS FS Measurement Counters for SIP Messages and Subscriber Features (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POTS_CFU_DEACTIVATION_ATTEMPTS</td>
<td>The number of Call Forward Unconditional deactivation attempts on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CFU_ACTIVATION_REFUSED</td>
<td>*The number of Call Forward Unconditional activations refused by the called party on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CFU_ACTIVATION_ANSWERED</td>
<td>The number of Call Forward Unconditional activations answered by the called party on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CFU_ACTIVATION_SECOND</td>
<td>The number of Call Forward Unconditional second attempt activations on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CFU_FORWARDED_FAIL</td>
<td>*The number of Call Forward Unconditional service instances that failed on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CFU_FORWARDED_SUCC</td>
<td>The number of Call Forward Unconditional service instances that succeeded on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CFB_ACTIVATION_ATTEMPTS</td>
<td>The number of Call Forward Busy activation attempts on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CFB_DEACTIVATION_ATTEMPTS</td>
<td>The number of Call Forward Busy deactivation attempts on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CFB_ACTIVATION_REFUSED</td>
<td>*The number of Call Forward Busy activations that were refused by the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CFB_FORWARDED_FAIL</td>
<td>*The number of Call Forward Busy service instances that failed on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CFB_FORWARDED_SUCC</td>
<td>The number of Call Forward Busy service instances that succeeded on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CFNA_ACTIVATION_ATTEMPTS</td>
<td>The number of Call Forward No Answer activations attempts on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CFNA_DEACTIVATION_ATTEMPTS</td>
<td>The number of Call Forward No Answer deactivation attempts on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CFNA_ACTIVATION_REFUSED</td>
<td>*The number of Call Forward No Answer activation that were refused by the reporting POTS Feature Server.</td>
</tr>
</tbody>
</table>
### Table 19-1 CA and POTS FS Measurement Counters for SIP Messages and Subscriber Features (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POTS_CFWA_FORWARDED_FAIL</td>
<td>*The number of Call Forward No Answer service instances that failed on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CFWA_FORWARDED_SUCCEED</td>
<td>The number of Call Forward No Answer service instances that succeeded on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CWA_ATTEMPTS</td>
<td>The number of Call Waiting service instance attempts handled by the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CWA_ANSWERED</td>
<td>The number of Call Waiting service instances that were answered by the called party on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CWA_NOT_ANSWERED</td>
<td>The number of Call Waiting service instances that were not answered by the called party on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CWA_REJECTED_NO_RESOURCES</td>
<td>*The number of Call Waiting service instances that were rejected due to a lack of available resources by the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CWA_REJECTED_INTERACTIONS</td>
<td>*The number of Call Waiting service instances that were rejected due to feature interaction by the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CCWA_ATTEMPTS</td>
<td>The total number of Cancel Call Waiting attempts on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CCWA_REJECTED_NO_RESOURCES</td>
<td>*The number of Cancel Call Waiting service instances that were rejected due to a lack of resources on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CCWA_REJECTED_BY_CCW</td>
<td>*The number of Cancel Call Waiting service instances that were rejected due to Call Waiting not already being active on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CCWA_LENGTH</td>
<td>The total time for all subscribers on the reporting POTS Feature Server that Cancel Call Waiting was active.</td>
</tr>
<tr>
<td>POTS_ANI_ATTEMPT_SUCCESS</td>
<td>The total number of Automatic Number Identification directory number lookups that were successfully attempted on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_ANI_BLOCKED_CALLS</td>
<td>The total number calls that were blocked based on Automatic Number Identification lookup on the reporting POTS Feature Server.</td>
</tr>
</tbody>
</table>
### List of Traffic Measurements (Counters)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POTS_NANP_BLOCKED_BW</td>
<td>The number of North American Numbering Plan based calls that were blocked due to a match on a black list or exclusion from a white list on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_INTL_BLOCKED_BW</td>
<td>The number of international based calls that were blocked due to a match on a black list or exclusion from a white list on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_900_RESTRICTED</td>
<td>The number of calls denied due to subscriber-based 900 restrictions on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_976_RESTRICTED</td>
<td>The number of calls denied due to subscriber-based 976 restrictions on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_NANP_RESTRICTED</td>
<td>The number of calls denied due to subscriber-based North American Numbering Plan restrictions on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_INTL_RESTRICTED</td>
<td>The number of calls denied due to subscriber-based international restrictions on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CASUAL_RESTRICTED</td>
<td>The number of calls denied due to subscriber-based casual dialing restrictions on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_DA_RESTRICTED</td>
<td>The number of calls denied due to subscriber-based directory assistance restrictions on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_NANP_OP_RESTRICTED</td>
<td>The number of calls denied due to subscriber-based NANP operator restrictions on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_INTL_OP_RESTRICTED</td>
<td>The number of calls denied due to subscriber-based international operator restrictions on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_AUTH_CODE_PASSED</td>
<td>The number of successful authentication code validations on the reporting POTS or CENTREX Feature Server.</td>
</tr>
<tr>
<td>POTS_AUTH_CODE_FAILED</td>
<td>*The number of unsuccessful authentication code validations on the reporting POTS or CENTREX Feature Server.</td>
</tr>
<tr>
<td>POTS_ACCT_CODE_PASSED</td>
<td>The number of successful account code validations on the reporting POTS or CENTREX Feature Server.</td>
</tr>
</tbody>
</table>
### Table 19-1 CA and POTS FS Measurement Counters for SIP Messages and Subscriber Features (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POTS_ACCT_CODE_FAILED</td>
<td>*The number of unsuccessful account code validations on the reporting POTS or CENTREX Feature Server.</td>
</tr>
<tr>
<td>POTS_CHD_ATTEMPTS</td>
<td>The number of Call Hold service instances on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CHD_ANSWERED</td>
<td>The number of Call Hold service instances that were reconnected on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CHD_NOT_ANSWERED</td>
<td>The number of Call Hold service instances that were not reconnected on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CHD_REJECTED_NO_RESOURCES</td>
<td>*The number of Call Hold service instances that were rejected due to a lack of resources on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CHD_REJECTED_INTERACTIONS</td>
<td>*The number of Call Hold service instances that were rejected due to feature interactions on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_MDC_ATTEMPTS</td>
<td>The number of midcall trigger attempts made by the subscribers on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_MDC_REJECTED_NO_RESOURCES</td>
<td>*The number of midcall trigger attempts made by the subscribers that were rejected due to no resources being available on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_MDC_REJECTED_INTERACTIONS</td>
<td>*The number of midcall trigger attempts made by the subscribers that were rejected due to feature interactions on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_MDC_REJECTED_OTHERS</td>
<td>*The number of midcall trigger attempts made by the subscribers that were rejected due to unknown reasons on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CT_ATTEMPTS</td>
<td>The number of Call Transfer service instances attempted on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CT_ANSWERED</td>
<td>The number of Call Transfer service instances answered by the called party on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CT_TRANSFERRED</td>
<td>The number of Call Transfer service instances resulting in a successfully transferred call on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_CT_CONFERENCED</td>
<td>The number of Call Transfer service instances resulting in the successful setup of a conference call on the reporting POTS Feature Server.</td>
</tr>
</tbody>
</table>
Table 19-1  CA and POTS FS Measurement Counters for SIP Messages and Subscriber Features (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POTS_CT_FAILED</td>
<td>&quot;The number of Call Transfer service instances attempts that failed on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_TWC_ATTEMPTS</td>
<td>The number of Three-Way Call service instances attempted on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_TWC_ANSWERED</td>
<td>The number of Three-Way Call service instances answered by the called party on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_TWC_CONFERENCED</td>
<td>The number of Three-Way Call service instances resulting in the successful setup of a conference call on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_TWC_FAILED</td>
<td>&quot;The number of Three-Way Call service instances attempts that failed on the reporting POTS Feature Server.</td>
</tr>
<tr>
<td>POTS_HOTLINE_ATTEMPT</td>
<td>The number of Hotline service instance attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_WARMLINE_ATTEMPT</td>
<td>The number of Warmline service instance attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_BLV_ATTEMPTS</td>
<td>The number of Busy Line Verification service instance attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_OPERATOR_INTERRUPT_ATTEMPTS</td>
<td>The number of Operator Interrupt service instance attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_SCR_ATTEMPTS</td>
<td>The number of Selective Call Rejection service instance attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_SCA_ATTEMPTS</td>
<td>The number of Selective Call Acceptance service instance attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_SCR_REJECTED_NO_RESOURCES</td>
<td>The number of Selective Call Rejection attempts made by subscribers that were rejected due to a lack of available resources on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_SCA_REJECTED_NO_RESOURCES</td>
<td>The number of Selective Call Acceptance attempts made by subscribers that were rejected due to a lack of available resources on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_SCR_SUCCESSFUL</td>
<td>The number of Selective Call Rejection service instance attempts resulting in successful rejections of the call on the reporting Feature Server.</td>
</tr>
</tbody>
</table>
### Table 19-1 CA and POTS FS Measurement Counters for SIP Messages and Subscriber Features (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POTS_SCA_SUCCESSFUL</td>
<td>The number of Selective Call Acceptance service instance attempts resulting in successful acceptance of the call on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_DRCW_ATTEMPTS</td>
<td>The number of Distinctive Ring Call Waiting service instance attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_DRCW_REJECTED_NO_RESOURCES</td>
<td>The number of Distinctive Ring Call Waiting attempts that were rejected due to a lack of available resources on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_DRCW_SUCCESSFUL</td>
<td>The number of Distinctive Ring Call Waiting attempts that were successful on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_SCF_ATTEMPTS</td>
<td>The number of Selective Call Forwarding service instance attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_SCF_REJECTED_NO_RESOURCES</td>
<td>The number of Selective Call Forwarding attempts that were rejected due to a lack of available resources on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_SCF_SUCCESSFUL</td>
<td>The number of Selective Call Forwarding attempts that were successful on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_COT_ACCESS</td>
<td>The number of times the Caller Originated Trace star code was dialed by the subscriber (feature accesses and activations).</td>
</tr>
<tr>
<td>POTS_COT_DENIED</td>
<td>Trace data was unsuccessfully accessed on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_COT_ACTIVATION</td>
<td>Same as POTS_COT_ACCESS in this release. When 2-level COT (the digit “1” dialed) is available, this counter would include both those and the current 1-level activations tracked in POTS_COT_ACCESS.</td>
</tr>
<tr>
<td>POTS_COT_ABANDONED</td>
<td>The number of Caller Originated Trace service activation abandonments that occurred on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_COT_DN_UNAVAILABLE</td>
<td>The number of Caller Originated Trace service activation that failed due to the calling party directory number not being available on the reporting Feature Server.</td>
</tr>
<tr>
<td>Measurement</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>POTS_COT_TRACE_CONFIRMED</td>
<td>The number of Caller Originated Trace service instances that were successfully completed on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_COT_TRACE_OUTPUT</td>
<td>The number of Caller Originated Trace service instances that were successfully completed and the data was stored persistently on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_RACF_ATTEMPTS</td>
<td>The number of Remote Activation Call Forward attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_RACF_REFUSED</td>
<td>The number of Remote Activation Call Forward service instances refused by the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_RACF_REJECTED_NO_RESOURCES</td>
<td>The number of Remote Activation Call Forward service instances refused due to a lack of available resources on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_RACF_CFU_ACTIVATED</td>
<td>The number of Remote Activation Call Forward activation attempts that were successful on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_RACF_CFU_DEACTIVATED</td>
<td>The number of Remote Activation Call Forward deactivation attempts that were successful on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_RACF_CFU_UNCHANGED</td>
<td>The number of Remote Activation Call Forward service instances that were successful but resulted in no change to the forwarding-to number on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_RACF_PIN_ATTEMPTS</td>
<td>The number of Remote Activation Call Forward PIN input attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_RACF_PIN_REFUSED</td>
<td>The number of Remote Activation Call Forward PIN input attempts that were refused on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_RACF_PIN_REJECTED_NO_RESOURCES</td>
<td>The number of Remote Activation Call Forward PIN input attempts that were refused due to a lack of resources on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_RACF_PIN_CHANGED</td>
<td>The number of Remote Activation Call Forward PIN input attempts that resulted in a change to the previous PIN for that subscriber on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_RACF_PIN_UNCHANGED</td>
<td>The number of Remote Activation Call Forward PIN input attempts that resulted in no change to the previous PIN for that subscriber on the reporting Feature Server.</td>
</tr>
</tbody>
</table>
Table 19-1 CA and POTS FS Measurement Counters for SIP Messages and Subscriber Features (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POTS_AC_ACTIVATION_ATTEMPTS</td>
<td>The number of Automatic Callback service activation attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_AC_OVERFLOWS</td>
<td>The number of Automatic Callback service activation attempts resulting in an overflow on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_AC_IMMEDIATE_PROCESSING</td>
<td>The number of Automatic Callback service activation attempts that resulted in immediate connection on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_AC_DELAYED_PROCESSING</td>
<td>The number of Automatic Callback service activation attempts that resulted in delayed connection on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_AC_DEACTIVATION_BY_SYSTEM</td>
<td>The number of Automatic Callback service activation attempts that were deactivated by the system on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_AC_DEACTIVATION_ATTEMPTS</td>
<td>The number of Automatic Callback service activation attempts that were deactivated by the requesting subscriber on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_AC_INTERLATA_ATTEMPTS</td>
<td>The number of Automatic Callback service activation attempts performed on an interlata basis on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_AR_ACTIVATION_ATTEMPTS</td>
<td>The number of Automatic Recall service activation attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_AR_OVERFLOWS</td>
<td>The number of Automatic Recall service activation attempts resulting in an overflow on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_AR_IMMEDIATE_PROCESSING</td>
<td>The number of Automatic Recall service activation attempts that resulted in immediate connection on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_AR_DELAYED_PROCESSING</td>
<td>The number of Automatic Recall service activation attempts that resulted in delayed connection on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_AR_DEACTIVATION_BY_SYSTEM</td>
<td>The number of Automatic Recall service activation attempts that were deactivated by the system on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_AR_DEACTIVATION_ATTEMPTS</td>
<td>The number of Automatic Recall service activation attempts that were deactivated by the requesting subscriber on the reporting Feature Server.</td>
</tr>
</tbody>
</table>

(* = rapid count can mean a potential problem in the system)
### Table 19-1 CA and POTS FS Measurement Counters for SIP Messages and Subscriber Features (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POTS_AR_INTERLATA_ATTEMPTS</td>
<td>The number of Automatic Recall service activation attempts performed on an interlata basis on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_ACART_QUEUE_REQUESTS</td>
<td>The number of Automatic Callback and Automatic Recall service requests that were queued on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_ACART_TERM_SCAN_REQUESTS</td>
<td>The number of Automatic Callback and Automatic Recall service requests that were queued for terminators on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_ACART_ORIG_SCAN_REQUESTS</td>
<td>The number of Automatic Callback and Automatic Recall service requests that were queued for originators on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_ACART_REJECT_NO_RESOURCES</td>
<td>The number of Automatic Callback and Automatic Recall service requests that were rejected due to a lack of resources on the reporting Feature Server.</td>
</tr>
<tr>
<td>CTX_SFG_COUNTER_OVERFLOW</td>
<td>The number of Centrex SFG counters that overflowed during the collection interval on the reporting Feature Server.</td>
</tr>
<tr>
<td>CTX_CPRK_SUCC_ATTEMPTS</td>
<td>The number of Call Park Attempts that were successful during the collection interval.</td>
</tr>
<tr>
<td>CTX_CPRK_FAIL_ATTEMPTS</td>
<td>The number of Call Park Attempts that failed during the collection interval.</td>
</tr>
<tr>
<td>CTX_CPRK_SUCC_RET_ATTEMPTS</td>
<td>The number of Call Park Retrieval Attempts that were successful during the collection interval.</td>
</tr>
<tr>
<td>CTX_CPRK_FAIL_RET_ATTEMPTS</td>
<td>The number of Call Park Retrieval Attempts that failed during the collection interval.</td>
</tr>
<tr>
<td>CTX_CPRK_FORWARDED</td>
<td>The number of Call Park Attempts to forward a call during the collection interval.</td>
</tr>
<tr>
<td>CTX_CPRK_CLEARED</td>
<td>The number of Call Park Attempts to clear during the collection interval.</td>
</tr>
<tr>
<td>POTS_SC_1_DIGIT_ATTEMPTS</td>
<td>The number of Speed Call 1 digit attempts during the collection interval.</td>
</tr>
<tr>
<td>POTS_SC_2_DIGIT_ATTEMPTS</td>
<td>The number of Speed Call 2 digit attempts during the collection interval.</td>
</tr>
<tr>
<td>POTS_SC_SUCC_CCSC</td>
<td>The number of CCSC successful attempts during the collection interval.</td>
</tr>
<tr>
<td>POTS_ACR_ACT_ATTEMPTS</td>
<td>The number of Automatic Call Return activation attempts during the collection interval.</td>
</tr>
</tbody>
</table>
### Table 19-1 CA and POTS FS Measurement Counters for SIP Messages and Subscriber Features (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POTS_ACR_DEACT_ATTEMPTS</td>
<td>The number of Automatic Call Return deactivation attempts during the collection interval.</td>
</tr>
<tr>
<td>POTS_ACR_ACT_REJECTED_NO_RESOURCES</td>
<td>The number of Automatic Call Return activation attempts that failed due to a lack of resources during the collection interval.</td>
</tr>
<tr>
<td>POTS_ACR_DEACT_REJECTED_NO_RESOURCES</td>
<td>The number of Automatic Call Return deactivation attempts during the collection interval.</td>
</tr>
<tr>
<td>POTS_ACR_SUCCESSFUL</td>
<td>The number of Automatic Call Return attempts that were successful during the collection interval.</td>
</tr>
<tr>
<td>POTS_DND_DEACT_REJECTED_NO_RESOURCES</td>
<td>The number of Do Not Disturb deactivation attempts during the collection interval.</td>
</tr>
<tr>
<td>POTS_DND_ACT_SUCCESS</td>
<td>The number of Do Not Disturb activation attempts during the collection interval.</td>
</tr>
<tr>
<td>POTS_DND_ACT_FAILURE</td>
<td>The number of Do Not Disturb deactivation attempts during the collection interval.</td>
</tr>
<tr>
<td>POTS_DND_DEACT_SUCCESS</td>
<td>The number of Do Not Disturb activation attempts that failed due to a lack of resources during the collection interval.</td>
</tr>
<tr>
<td>POTS_DND_DEACT_FAILURE</td>
<td>The number of Do Not Disturb deactivation attempts during the collection interval.</td>
</tr>
<tr>
<td>POTS_DND_REJECTION</td>
<td>The number of Do Not Disturb activation attempts rejected during the collection interval.</td>
</tr>
<tr>
<td>POTS_RC_SUCCESSFUL</td>
<td>The number of Return Call attempts that were successful during the collection interval.</td>
</tr>
<tr>
<td>POTS_CWD_ATTEMPTS</td>
<td>The number of Call Waiting Deluxe service instance attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_CWD_ANSWERED</td>
<td>The number of Call Waiting Deluxe service instance attempts answered by the called party on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_CWD_ACTIVATION_SUCC</td>
<td>The number of Call Waiting Deluxe successful service activation attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_CWD_ACTIVATION_FAIL</td>
<td>The number of Call Waiting Deluxe unsuccessful service activation attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_CWD_DEACTIVATION_SUCC</td>
<td>The number of Call Waiting Deluxe successful service deactivation attempts on the reporting Feature Server.</td>
</tr>
</tbody>
</table>
### Table 19-1 CA and POTS FS Measurement Counters for SIP Messages and Subscriber Features (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POTS_CWD_DEACTIVATION_FAIL</td>
<td>The number of Call Waiting Deluxe unsuccessful service deactivation attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_CWD_INTERROGATION_SUCC</td>
<td>The number of Call Waiting Deluxe successful service interrogation attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_CWD_INTERROGATION_FAIL</td>
<td>The number of Call Waiting Deluxe unsuccessful service interrogation attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_TWCD_ATTEMPTS</td>
<td>The number of Three-Way Calling Deluxe service instance attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_TWCD_CONFERENCED</td>
<td>The number of Three-Way Calling Deluxe service instance conferencing attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_OCB_LOCAL_BLOCKED</td>
<td>The number of local calls that were blocked on the reporting Feature Server via Outward Call Barring.</td>
</tr>
<tr>
<td>POTS_OCB_NATL_BLOCKED</td>
<td>The number of national calls that were blocked on the reporting Feature Server via Outward Call Barring.</td>
</tr>
<tr>
<td>POTS_OCB_INTL_BLOCKED</td>
<td>The number of international calls that were blocked on the reporting Feature Server via Outward Call Barring.</td>
</tr>
<tr>
<td>POTS_OCB_INVOCATIONS</td>
<td>The number of Outward Call Barring invocation attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_OCBActivation_SUCC</td>
<td>The number of Outward Call Barring successful activation attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_OCBDEACTIVATION_SUCC</td>
<td>The number of Outward Call Barring successful deactivation attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_OCB_INTERROGATION_SUCC</td>
<td>The number of Outward Call Barring successful interrogation attempts on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_OCB_INVALID_PASSWORD</td>
<td>The number of Outward Call Barring attempts that were unsuccessful due to invalid password entry by the user on the reporting Feature Server.</td>
</tr>
<tr>
<td>POTS_HOTV_ATTEMPTS</td>
<td>The number of successful Hotline Variable instance attempts on the reporting Feature Server.</td>
</tr>
</tbody>
</table>
List of Traffic Measurements (Counters)

Table 19-2 describes the Subscriber feature measurement counters for AIN FS.

Table 19-2  AIN FS Measurements

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_TOTAL_INCOMING_MSG</td>
<td>The number of SIP messages the reporting Call Agent or Feature Server attempted to receive.</td>
</tr>
<tr>
<td>SIP_TOTAL_SUCCESS_INCOMING_MSG</td>
<td>The number of SIP messages the reporting Call Agent or Feature Server successfully received.</td>
</tr>
<tr>
<td>Measurement/Counter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SIP_TOTAL_OUTGOING_MSG</td>
<td>The number of SIP messages the reporting Call Agent or Feature Server attempted to send.</td>
</tr>
<tr>
<td>SIP_TOTAL_SUCCESS_OUTGOING_MSG</td>
<td>The number of SIP messages the reporting Call Agent or Feature Server successfully sent.</td>
</tr>
<tr>
<td>SIP_REQ_RETRAN_RCVD</td>
<td>The number of SIP request retransmission messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_REQ_RETRAN_SENT</td>
<td>The number of SIP request retransmission messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_RSP_RETRAN_RCVD</td>
<td>The number of SIP response retransmission messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_RSP_RETRAN_SENT</td>
<td>The number of SIP response retransmission messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_T1 TIMER_EXPIRED</td>
<td>The number of SIP T1 Timer expirations that occurred on the reporting Call Agent or Feature Server received over the collection interval.</td>
</tr>
<tr>
<td>SIP_T2 TIMER_REACHED</td>
<td>The number of SIP T2 Timer expirations that occurred on the reporting Call Agent or Feature Server received over the collection interval.</td>
</tr>
<tr>
<td>SIP_INVITE_RECEIVED</td>
<td>The number of SIP INVITE messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_INVITE_SENT</td>
<td>The number of SIP INVITE messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_CANCEL_RECEIVED</td>
<td>The number of SIP CANCEL messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_CANCEL_SENT</td>
<td>The number of SIP CANCEL messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_BYE_RECEIVED</td>
<td>The number of SIP BYE messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_BYE_SENT</td>
<td>The number of SIP BYE messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_ACK_RECEIVED</td>
<td>The number of SIP ACK messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_ACK_SENT</td>
<td>The number of SIP ACK messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_OPTIONS_RECEIVED</td>
<td>The number of SIP OPTIONS messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>Measurement/Counter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SIP_OPTIONS_SENT</td>
<td>The number of SIP OPTIONS messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_REGISTER_RECEIVED</td>
<td>The number of SIP REGISTER messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_REGISTER_SENT</td>
<td>The number of SIP REGISTER messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_INFO_RECEIVED</td>
<td>The number of SIP INFO messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_INFO_SENT</td>
<td>The number of SIP INFO messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_NOTIFY_RECEIVED</td>
<td>The number of SIP NOTIFY messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_NOTIFY_SENT</td>
<td>The number of SIP NOTIFY messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_100_RECEIVED</td>
<td>The number of 100 class (TRYING) messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_100_SENT</td>
<td>The number of 100 class (TRYING) messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_18x_RECEIVED</td>
<td>The number of 18x class (INFORMATIONAL) messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_18x_SENT</td>
<td>The number of 18x class (INFORMATIONAL) messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_200_RECEIVED</td>
<td>The number of 200 class (SUCCESS) messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_200_SENT</td>
<td>The number of 200 class (SUCCESS) messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_3xx_RECEIVED</td>
<td>The number of 3xx class (REDIRECTION) messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_3xx_SENT</td>
<td>The number of 3xx class (REDIRECTION) messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_4xx_RECEIVED</td>
<td>The number of 4xx class (REQUEST FAILURES) messages the reporting Call Agent or Feature Server received.</td>
</tr>
</tbody>
</table>
Table 19-2  AIN FS Measurements (continued)

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_4xx_SENT</td>
<td>The number of 4xx class (REQUEST FAILURES) messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_5xx_RECEIVED</td>
<td>The number of 5xx class (SERVER FAILURES) messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_5xx_SENT</td>
<td>The number of 5xx class (SERVER FAILURES) messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_6xx_RECEIVED</td>
<td>The number of 6xx class (GLOBAL FAILURES) messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_6xx_SENT</td>
<td>The number of 6xx class (GLOBAL FAILURES) messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_7xx_RECEIVED</td>
<td>The number of 7xx class (RESERVED) messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_7xx_SENT</td>
<td>The number of 7xx class (RESERVED) messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_PROV_RSP_RETRAN_RCVD</td>
<td>The number of SIP provisioning response retransmission messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_PROV_RSP_RETRAN_SENT</td>
<td>The number of SIP provisioning response retransmission messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_PRACK_RECEIVED</td>
<td>The number of SIP PRACK messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_PRACK_SENT</td>
<td>The number of SIP PRACK messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_SUBSCRIBE_RECEIVED</td>
<td>The number of SIP SUBSCRIBE messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_SUBSCRIBE_SENT</td>
<td>The number of SIP SUBSCRIBE messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIPREFER_RECEIVED</td>
<td>The number of SIP REFER messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIPREFER_SENT</td>
<td>The number of SIP REFER messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIPREFER_REPLACES_RECEIVED</td>
<td>The number of SIP REFER REPLACES messages the reporting Call Agent or Feature Server received.</td>
</tr>
</tbody>
</table>
### List of Traffic Measurements (Counters)

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_INVITE_REPLACES_SENT</td>
<td>The number of SIP INVITE REPLACES messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_INVITE_REPLACES_RECEIVED</td>
<td>The number of SIP INVITE REPLACES messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_REL100_RECEIVED</td>
<td>The number of REL100 class (TRYING) messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_REL100_SENT</td>
<td>The number of REL100 class (TRYING) messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_UNSUPPORTED_RECEIVED</td>
<td>The number of unsupported SIP messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>NUM_OF_AIN</td>
<td>The number of queries attempted on the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>NUM_OF_8XX</td>
<td>The number of 8XX translation queries attempted on the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>NUM_OF_EXT_8XX</td>
<td>The number of 8XX translation queries that resulted in an external query to a network database attempted from the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>NUM_OF_EXT_8XX_SUCCEED</td>
<td>The number of 8XX translation queries that resulted in a successful external query to a network database from the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>NUM_OF_EXT_8XX_FAIL_APPL</td>
<td><em>The number of 8XX translation queries that resulted in a failed external query to a network database due to an application error from the reporting AIN Feature Server.</em></td>
</tr>
<tr>
<td>NUM_OF_EXT_8XX_FAIL_NET</td>
<td><em>The number of 8XX translation queries that resulted in a failed external query to a network database due to a network communication error from the reporting AIN Feature Server.</em></td>
</tr>
<tr>
<td>NUM_OF_LOC_8XX</td>
<td>The number of 8XX translation queries attempted to be processed locally on the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>NUM_OF_LOC_8XX_SUCCEED</td>
<td>The number of 8XX translation queries that were successfully processed locally on the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>NUM_OF_LOC_8XX_ANI_BLOCKED</td>
<td>The number of 8XX translation queries that were blocked due to ANI screening processed locally on the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>Measurement/Counter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NUM_OF_LOC_8XX_II_BLOCKED</td>
<td>The number of 8XX translation queries that were blocked due to II screening processed locally on the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>NUM_OF_LOC_8XX_DNIS_SUCCEED</td>
<td>The number of 8XX DNIS translation queries that were successfully processed locally on the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>NUM_OF_LOC_8XX_ROUTING_SUCCEED</td>
<td>The number of 8XX routing translation queries that were successfully processed locally on the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>NUM_OF_LOC_8XX_REROUTED</td>
<td>The number of 8XX translation queries that were successfully processed locally on the reporting AIN Feature Server that resulted in re-routing.</td>
</tr>
<tr>
<td>NUM_OF_LOC_8XX_FAIL_APPL</td>
<td>*The number of 8XX translation queries that resulted in a failure due to a local application error from the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>NUM_OF_LNP</td>
<td>The total number of Local Number Portability translation queries attempted on the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>NUM_OF_EXT_LNP</td>
<td>The number of Local Number Portability translation queries that resulted in queries to network databases from the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>NUM_OF_EXT_LNP_SUCCEED</td>
<td>The number of Local Number Portability translation queries that resulted in successful queries to network databases from the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>NUM_OF_EXT_LNP_FAIL_APPL</td>
<td>*The number of Local Number Portability translation queries that resulted in failed queries to network databases due to application error from the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>NUM_OF_EXT_LNP_FAIL_NET</td>
<td>*The number of Local Number Portability translation queries that resulted in failed queries to network databases due to network error from the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>NUM_OF_CNAM</td>
<td>The number of Calling Name queries attempted on the reporting AIN Feature Server.</td>
</tr>
<tr>
<td>NUM_OF_EXT_CNAM</td>
<td>The number of Calling Name queries attempted that resulted in queries to network databases from the reporting AIN Feature Server.</td>
</tr>
</tbody>
</table>
### Service Interaction Manager Counters

Table 19-3 describes the measurement counters for the Service Interaction Manager (SIM).

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
<th>(*=rapid count can mean a potential problem in the system)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_TOTAL_INCOMING_MSG</td>
<td>The total number of SIP messages that the reporting Call Agent attempted to receive.</td>
<td></td>
</tr>
<tr>
<td>SIP_TOTAL_SUCCESS_INCOMING_MSG</td>
<td>The total number of SIP messages successfully received by the reporting Call Agent.</td>
<td></td>
</tr>
<tr>
<td>SIP_TOTAL_OUTGOING_MSG</td>
<td>The total number of SIP messages that the reporting Call Agent attempted to transmit.</td>
<td></td>
</tr>
<tr>
<td>SIP_TOTAL_SUCCESS_OUTGOING_MSG</td>
<td>The total number of SIP messages that the reporting Call Agent successfully transmitted.</td>
<td></td>
</tr>
<tr>
<td>SIP_REQ RETRAN_RCVD</td>
<td>The total number of SIP request retransmission messages received by the reporting Call Agent or Feature Server.</td>
<td></td>
</tr>
<tr>
<td>SIP_REQ RETRAN_SENT</td>
<td>The total number of SIP request retransmission messages transmitted by the reporting Call Agent or Feature Server.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 19-3  Service Interaction Manager (SIM) Measurement Counters (continued)

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_RSP_RETRAN_RCVD</td>
<td>The total number of SIP response retransmission messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_RSP_RETRAN_SENT</td>
<td>The total number of SIP response retransmission messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_T1_TIMER_EXPIRED</td>
<td>*The total number of T1 Timer expirations that occurred during the current collection interval on the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_T2_TIMER_REACHED</td>
<td>*The total number of T2 Timer expirations that occurred during the current collection interval on the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_INVITE_RECEIVED</td>
<td>The total number of INVITE messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_INVITE_SENT</td>
<td>The total number of INVITE messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_CANCEL_RECEIVED</td>
<td>The total number of CANCEL messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_CANCEL_SENT</td>
<td>The total number of CANCEL messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_BYE_RECEIVED</td>
<td>The total number of BYE messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_BYE_SENT</td>
<td>The total number of BYE messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_ACK_RECEIVED</td>
<td>The total number of ACK messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_ACK_SENT</td>
<td>The total number of ACK messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_OPTIONS_RECEIVED</td>
<td>The total number of OPTION messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_OPTIONS_SENT</td>
<td>The total number of OPTION messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_REGISTER_RECEIVED</td>
<td>The total number of REGISTER messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_REGISTER_SENT</td>
<td>The total number of REGISTER messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_INFO_RECEIVED</td>
<td>The total number of INFO messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_INFO_SENT</td>
<td>The total number of INFO messages transmitted by the reporting Call Agent.</td>
</tr>
</tbody>
</table>
### Table 19-3  Service Interaction Manager (SIM) Measurement Counters (continued)

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_NOTIFY_RECEIVED</td>
<td>The total number of NOTIFY messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_NOTIFY_SENT</td>
<td>The total number of NOTIFY messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_100_RECEIVED</td>
<td>The total number of 100 (trying) messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_100_SENT</td>
<td>The total number of 100 (trying) messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_18x_RECEIVED</td>
<td>The total number of 18x (informational) messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_18x_SENT</td>
<td>The total number of 18x (informational) messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_200_RECEIVED</td>
<td>The total number of 200 (success) messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_200_SENT</td>
<td>The total number of 200 (success) messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_3xx_RECEIVED</td>
<td>The total number of 3xx (redirection) messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_3xx_SENT</td>
<td>The total number of 3xx (redirection) messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_4xx_RECEIVED</td>
<td>*The total number of 4xx (request failures) messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_4xx_SENT</td>
<td>*The total number of 4xx (request failures) messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_5xx_RECEIVED</td>
<td>*The total number of 5xx (server failures) messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_5xx_SENT</td>
<td>*The total number of 5xx (server failures) messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_6xx_RECEIVED</td>
<td>*The total number of 6xx (global failures) messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_6xx_SENT</td>
<td>*The total number of 6xx (global failures) messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_7xx_RECEIVED</td>
<td>The total number of 7xx (reserved) messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_7xx_SENT</td>
<td>The total number of 7xx (reserved) messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_PROV_RSP_RETRAN_RCVD</td>
<td>The number of SIP provisioning response retransmission messages the reporting Call Agent or Feature Server received.</td>
</tr>
</tbody>
</table>

(*)=rapid count can mean a potential problem in the system
### Table 19-3  Service Interaction Manager (SIM) Measurement Counters (continued)

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_PROV_RSP_RETRAN_SENT</td>
<td>The number of SIP provisioning response retransmission messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_PRACK_RECEIVED</td>
<td>The number of SIP PRACK messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_PRACK_SENT</td>
<td>The number of SIP PRACK messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_SUBSCRIBE_RECEIVED</td>
<td>The number of SIP SUBSCRIBE messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_SUBSCRIBE_SENT</td>
<td>The number of SIP SUBSCRIBE messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIPREFER_RECEIVED</td>
<td>The number of SIP REFER messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIPREFER_SENT</td>
<td>The number of SIP REFER messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIPREFER_REPLACES_RECEIVED</td>
<td>The number of SIP REFER REPLACES messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_INVITE_REPLACES_SENT</td>
<td>The number of SIP INVITE REPLACES messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_INVITE_REPLACES_RECEIVED</td>
<td>The number of SIP INVITE REPLACES messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_REL100_RECEIVED</td>
<td>The number of REL100 class (TRYING) messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_REL100_SENT</td>
<td>The number of REL100 class (TRYING) messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_UNSUPPORTED_RECEIVED</td>
<td>The number of unsupported SIP messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>BCM_MESSAGES_CTR</td>
<td>The number of messages received by call processing in the reporting Call Agent from a Feature Server.</td>
</tr>
<tr>
<td>RELATIONS_CTR</td>
<td>The number of TDP-Rs received from call processing by the SIM on the reporting Call Agent.</td>
</tr>
<tr>
<td>TDP_N_CTR</td>
<td>The number of Trigger Detection Point messages received from call processing on the reporting Call Agent that do not require a response from the target Feature Server.</td>
</tr>
</tbody>
</table>
### Table 19-3  Service Interaction Manager (SIM) Measurement Counters (continued)

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TDP_R_CTR</td>
<td>The number of Trigger Detection Point messages received from call processing on the reporting Call Agent that do require a response from the target Feature Server.</td>
</tr>
<tr>
<td>EDP_N_CTR</td>
<td>The number of Event Detection Point messages received from call processing on the reporting Call Agent that do not require a response from the target Feature Server.</td>
</tr>
<tr>
<td>EDP_R_CTR</td>
<td>The number of Event Detection Point messages received from call processing on the reporting Call Agent that do require a response from the target Feature Server.</td>
</tr>
<tr>
<td>INSTRUCT_CTR</td>
<td>The number of INSTRUCT messages sent to Feature Servers by this Call Agent.</td>
</tr>
<tr>
<td>INSTRUCT_RESPONSE_CTR</td>
<td>The number of INSTRUCT messages received by call processing on the reporting Call Agent from Feature Servers.</td>
</tr>
<tr>
<td>TERMINATE_RECEIVED_CTR</td>
<td>The number of TERMINATE messages received by call processing on the reporting Call Agent from Feature Servers.</td>
</tr>
<tr>
<td>TERMINATE_SENT_CTR</td>
<td>The number of TERMINATE messages sent by call processing on the reporting Call Agent to Feature Servers.</td>
</tr>
<tr>
<td>FS_MESSAGES_SENT_CTR</td>
<td>The number of FCP messages sent to Feature Servers by the reporting Call Agent.</td>
</tr>
<tr>
<td>FS_MESSAGES RECEIVED_CTR</td>
<td>The total number of FCP messages received by call processing from the Feature Server by this Call Agent.</td>
</tr>
<tr>
<td>FS_PING_MESSAGES_SENT_CTR</td>
<td>The number Feature Server PING messages sent by call processing to Feature Servers by this Call Agent.</td>
</tr>
<tr>
<td>FS_PING_NO_RESPONSE_FAULTY_CTR</td>
<td>*The number of times that no response to a PING message was received from the Feature Servers by this Call Agent.</td>
</tr>
<tr>
<td>CA_RESTART_MESSAGES_SENT_CTR</td>
<td>*The number of Call Agent RESTART messages sent to the Feature Servers by the reporting Call Agent.</td>
</tr>
<tr>
<td>CA_ASYNC_MESSAGES_SENT_CTR</td>
<td>Number of Asynchronous Response Messages from BCM.</td>
</tr>
</tbody>
</table>
### MGCP Adapter Measurement Counters

Table 19-4 describes the Media Gateway Control Protocol (MGCP) Adapter (MGA) measurement counters.

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGA_TPM_DECODE_ERROR</td>
<td>*The number of MGCP messages received on the reporting Call Agent that failed decoding.</td>
</tr>
<tr>
<td>MGA_TPM_ENCODE_ERROR</td>
<td>*The number of MGCP messages to be sent from the reporting Call Agent that failed encoding.</td>
</tr>
<tr>
<td>MGA_TPM_UNREACHABLE</td>
<td>*The number of MGCP messages sent from the reporting Call Agent that failed due to the target gateway being unreachable.</td>
</tr>
<tr>
<td>MGA_TPM_SEND_FAILED</td>
<td>*The number of MGCP sent from the reporting Call Agent that failed when being sent to the target gateway.</td>
</tr>
<tr>
<td>MGA_TPM_CRCX_ACK_RECVD</td>
<td>The number of MGCP CRCX acknowledgments received by the reporting Call Agent.</td>
</tr>
<tr>
<td>MGA_TPM_CRCX_NACK_RECVD</td>
<td>*The number of MGCP CRCX nonacknowledgments received by the reporting Call Agent.</td>
</tr>
<tr>
<td>MGA_TPM_CRCX_SENT</td>
<td>The number of MGCP CRCX messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>MGA_TPM_MDCX_ACK_RECVD</td>
<td>The number of MGCP MDCX acknowledgments received by the reporting Call Agent.</td>
</tr>
<tr>
<td>MGA_TPM_MDCX_NACK_RECVD</td>
<td>*The number of MGCP MDCX nonacknowledgements received by the reporting Call Agent.</td>
</tr>
<tr>
<td>MGA_TPM_MDCX_SENT</td>
<td>The number of MGCP MDCX messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>MGA_TPM_DL CX_RECVD</td>
<td>The number of MGCP DLCX messages received from gateways by the reporting Call Agent.</td>
</tr>
<tr>
<td>MGA_TPM_DL CX_SENT</td>
<td>The number of MGCP DLCX messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>MGA_TPM_DL CX_ACK_RECVD</td>
<td>The number of MGCP DLCX acknowledgments received by the reporting Call Agent.</td>
</tr>
<tr>
<td>MGA_TPM_RQNT_ACK_RECVD</td>
<td>*The number of MGCP DLCX nonacknowledgments received by the reporting Call Agent.</td>
</tr>
<tr>
<td></td>
<td>The number of MGCP RQNT acknowledgments received by the reporting Call Agent.</td>
</tr>
</tbody>
</table>
Table 19-4  MGCP Adapter Measurement Counters (continued)

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGA_TPM_RQNT_NACK_RECV</td>
<td>*The number of MGCP RQNT nonacknowledgments received by the reporting Call Agent.</td>
</tr>
<tr>
<td>MGA_TPM_RQNT_SENT</td>
<td>The number of MGCP RQNT messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>MGA_TPM_AUEP_ACK_RECV</td>
<td>The number of MGCP AUEP acknowledgments received by the reporting Call Agent.</td>
</tr>
<tr>
<td>MGA_TPM_AUEP_NACK_RECV</td>
<td>*The number of MGCP AUEP nonacknowledgments received by the reporting Call Agent.</td>
</tr>
<tr>
<td>MGA_TPM_AUEP_SENT</td>
<td>The number of MGCP AUEP messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>MGA_TPM_NTFY_RECV</td>
<td>The number of MGCP NTFY messages received from gateways by the reporting Call Agent.</td>
</tr>
<tr>
<td>MGA_TPM_RSIP_RECV</td>
<td>The number of MGCP RSIP messages received from gateways by the reporting Call Agent.</td>
</tr>
<tr>
<td>MGA_TPM_RSIP_ACK_SENT</td>
<td>The number of MGCP RSIP message acknowledgments sent to the gateways from the reporting Call Agent.</td>
</tr>
</tbody>
</table>

**ISUP Measurement Counters**

Table 19-5 describes the ISDN User Part (ISUP) measurement counters.

Table 19-5  ISUP Measurement Counters

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S7A_TPM_IAM_RX</td>
<td>The total number of ISUP IAMs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_IAM_TX</td>
<td>The total number of ISUP IAMs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_ACM_RX</td>
<td>The total number of ISUP ACMs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_ACM_TX</td>
<td>The total number of ISUP ACMs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_ANM_RX</td>
<td>The total number of ISUP ANMs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_ANM_TX</td>
<td>The total number of ISUP ANMs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
</tbody>
</table>
### Table 19-5  ISUP Measurement Counters (continued)

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S7A_TPM_CPG_RX</td>
<td>The total number of ISUP CPGs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_CPG_TX</td>
<td>The total number of ISUP CPGs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_REL_RX</td>
<td>The total number of ISUP RELs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_REL_TX</td>
<td>The total number of ISUP RELs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_RLC_RX</td>
<td>The total number of ISUP RLCs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_RLC_TX</td>
<td>The total number of ISUP RLCs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_RSC_RX</td>
<td>The total number of ISUP RSCs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_RSC_TX</td>
<td>The total number of ISUP RSCs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_GRS_RX</td>
<td>The total number of ISUP GRSs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_GRS_TX</td>
<td>The total number of ISUP GRSs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_GRA_RX</td>
<td>The total number of ISUP GRAs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_GRA_TX</td>
<td>The total number of ISUP GRAs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_BLO_RX</td>
<td>*The total number of ISUP BLOs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_BLO_TX</td>
<td>The total number of ISUP BLOs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_BLA_RX</td>
<td>The total number of ISUP BLAs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_BLA_TX</td>
<td>The total number of ISUP BLAs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_UBL_RX</td>
<td>The total number of ISUP UBLs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_UBL_TX</td>
<td>The total number of ISUP UBLs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_UBA_RX</td>
<td>The total number of ISUP UBAs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_UBA_TX</td>
<td>The total number of ISUP UBAs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
</tbody>
</table>
### Table 19-5 ISUP Measurement Counters (continued)

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description (*=rapid count can mean a potential problem in the system)</th>
</tr>
</thead>
<tbody>
<tr>
<td>S7A_TPM_CGB_RX</td>
<td>*The total number of ISUP CGBs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_CGB_TX</td>
<td>The total number of ISUP CGBs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_CGBA_RX</td>
<td>The total number of ISUP CGBAs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_CGBA_TX</td>
<td>The total number of ISUP CGBAs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_CGU_RX</td>
<td>The total number of ISUP CGUs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_CGU_TX</td>
<td>The total number of ISUP CGUs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_CGUA_RX</td>
<td>The total number of ISUP CGUAs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_CGUA_TX</td>
<td>The total number of ISUP CGUAs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_MSU_TX</td>
<td>The total number of message signal units transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_MSU_RX</td>
<td>The total number of message signal units received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_MSU_TXRX</td>
<td>The total number of message signal units transmitted and received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_MSU8_TX</td>
<td>The total number of MSU octets transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_MSU8_RX</td>
<td>The total number of MSU octets received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_MSU8_TXRX</td>
<td>The total number of MSU octets transmitted and received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_MSU8_RETX</td>
<td>The total number of MSU octets retransmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_CVT_RX</td>
<td>The total number of ISUP CVTs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_CVT_TX</td>
<td>The total number of ISUP CVTs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_CVR_RX</td>
<td>The total number of ISUP CVRs received via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
<tr>
<td>S7A_TPM_CVR_TX</td>
<td>The total number of ISUP CVRs transmitted via the SS7 link(s) by the reporting Call Agent.</td>
</tr>
</tbody>
</table>
# Call Processing Measurement Counters

Table 19-6 describes the call processing measurement counters.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM_ORIG_ATTMP</td>
<td>The total number of originating call attempts of all types on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_TERM_ATTMP</td>
<td>The total number of terminating call attempts of all types on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_ORIG_FAIL</td>
<td>*The total number of originating call attempts of all types that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_TERM_FAIL</td>
<td>*The total number of terminating call attempts of all types that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_CALL_SUCC</td>
<td>The total number of successful originating and terminating calls of all types on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_CALL_ABAND</td>
<td>The total number of originating calls of all types that were abandoned on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_ISDN_ORIG_ATTMP</td>
<td>The total number of originating ISDN call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_ISDN_TERM_ATTMP</td>
<td>The total number of terminating ISDN call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_ISDN_ORIG_FAIL</td>
<td>*The total number of originating ISDN call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_ISDN_TERM_FAIL</td>
<td>*The total number of terminating ISDN call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_ISDN_CALL_SUCC</td>
<td>The total number of successful originating and terminating ISDN calls on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_ISDN_CALL_ABAND</td>
<td>The total number of originating ISDN calls that were abandoned on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SS7_ORIG_ATTMP</td>
<td>The total number of originating SS7 call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SS7_TERM_ATTMP</td>
<td>The total number of terminating SS7 call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SS7_ORIG_FAIL</td>
<td>*The total number of originating SS7 call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SS7_TERM_FAIL</td>
<td>*The total number of terminating SS7 call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SS7_CALL_SUCC</td>
<td>The total number of successful originating and terminating SS7 calls on the reporting Call Agent.</td>
</tr>
</tbody>
</table>
### Table 19-6 Call Processing Measurements (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM_SS7_CALL_ABAND</td>
<td>The total number of originating SS7 calls that were abandoned on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SIP_ORIG_ATTMP</td>
<td>The total number of originating SIP call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SIP_TERM_ATTMP</td>
<td>The total number of terminating SIP call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SIP_ORIG_FAIL</td>
<td>*The total number of originating SIP call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SIP_TERM_FAIL</td>
<td>*The total number of terminating SIP call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SIP_CALL_SUCC</td>
<td>The total number of successful originating and terminating SIP calls on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SIP_CALL_ABAND</td>
<td>The total number of originating SIP calls that were abandoned on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_MGCP_ORIG_ATTMP</td>
<td>The total number of originating MGCP call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_MGCP_TERM_ATTMP</td>
<td>The total number of terminating MGCP call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_MGCP_ORIG_FAIL</td>
<td>*The total number of originating MGCP call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_MGCP_TERM_FAIL</td>
<td>*The total number of terminating MGCP call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_MGCP_CALL_SUCC</td>
<td>The total number of successful originating and terminating MGCP calls on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_MGCP_CALL_ABAND</td>
<td>The total number of originating SIP calls that were abandoned on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_CAS_ORIG_ATTMP</td>
<td>The total number of originating CAS call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_CAS_TERM_ATTMP</td>
<td>The total number of terminating CAS call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_CAS_ORIG_FAIL</td>
<td>*The total number of originating CAS call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_CAS_TERM_FAIL</td>
<td>*The total number of terminating CAS call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_CAS_CALL_SUCC</td>
<td>The total number of successful originating and terminating CAS calls on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_CAS_CALL_ABAND</td>
<td>The total number of originating CAS calls that were abandoned on the reporting Call Agent.</td>
</tr>
</tbody>
</table>
### Table 19-6 Call Processing Measurements (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM_ISDN_SS7_CALL</td>
<td>The total number of successfully completed calls from an ISDN originator to an SS7 termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_ISDN_ISDN_CALL</td>
<td>The total number of successfully completed calls from an ISDN originator to an ISDN termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_ISDN_SIP_CALL</td>
<td>The total number of successfully completed calls from an ISDN originator to a SIP termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_ISDN_MGCP_CALL</td>
<td>The total number of successfully completed calls from an ISDN originator to an MGCP termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_ISDN_CAS_CALL</td>
<td>The total number of successfully completed calls from an ISDN originator to a CAS termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SS7_ISDN_CALL</td>
<td>The total number of successfully completed calls from an SS7 originator to an ISDN termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SS7_SS7_CALL</td>
<td>The total number of successfully completed calls from an SS7 originator to an SS7 termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SS7_SIP_CALL</td>
<td>The total number of successfully completed calls from an SS7 originator to a SIP termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SS7_MGCP_CALL</td>
<td>The total number of successfully completed calls from an SS7 originator to an MGCP termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SS7_CAS_CALL</td>
<td>The total number of successfully completed calls from an SS7 originator to a CAS termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SIP_SS7_CALL</td>
<td>The total number of successfully completed calls from a SIP originator to an SS7 termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SIP_ISDN_CALL</td>
<td>The total number of successfully completed calls from a SIP originator to an ISDN termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SIP_SIP_CALL</td>
<td>The total number of successfully completed calls from a SIP originator to a SIP termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SIP_MGCP_CALL</td>
<td>The total number of successfully completed calls from a SIP originator to an MGCP termination on the reporting Call Agent.</td>
</tr>
</tbody>
</table>
Table 19-6  Call Processing Measurements (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM_SIP_CAS_CALL</td>
<td>The total number of successfully completed calls from a SIP originator to a CAS termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_MGCP_SIP_CALL</td>
<td>The total number of successfully completed calls from an MGCP originator to a SIP termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_MGCP_ISDN_CALL</td>
<td>The total number of successfully completed calls from an MGCP originator to an ISDN termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_MGCP_SS7_CALL</td>
<td>The total number of successfully completed calls from an MGCP originator to an SS7 termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_MGCP_MGCP_CALL</td>
<td>The total number of successfully completed calls from an MGCP originator to an MGCP termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_MGCP_CAS_CALL</td>
<td>The total number of successfully completed calls from an MGCP originator to a CAS termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_CAS_SIP_CALL</td>
<td>The total number of successfully completed calls from a CAS originator to a SIP termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_CAS_ISDN_CALL</td>
<td>The total number of successfully completed calls from a CAS originator to an ISDN termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_CAS_SS7_CALL</td>
<td>The total number of successfully completed calls from a CAS originator to an SS7 termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_CAS_MGCP_CALL</td>
<td>The total number of successfully completed calls from a CAS originator to an MGCP termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_CAS_CAS_CALL</td>
<td>The total number of successfully completed calls from a CAS originator to a CAS termination on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_INTERLA_ATTMP</td>
<td>The total number of interlata call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_INTERLA_FAIL</td>
<td>*The total number of interlata call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_INTERLA_CALL_SUCU</td>
<td>The total number of successful interlata calls on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_INTERLA_CALL_ABAND</td>
<td>The total number of interlata calls that were abandoned on the reporting Call Agent.</td>
</tr>
<tr>
<td>Measurement</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>BCM_INTRALA_ATTMP</td>
<td>The total number of intralata call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_INTRALA_FAIL</td>
<td>*The total number of intralata call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_INTRAL_CALL_SUCC</td>
<td>The total number of successful intralata calls on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_INTRAL_CALL_ABAND</td>
<td>The total number of intralata calls that were abandoned on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_INTL_ATTMP</td>
<td>The total number of international call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_INTL_FAIL</td>
<td>*The total number of international call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_INTL_CALL_SUCC</td>
<td>The total number of successful international calls on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_INTL_CALL_ABAND</td>
<td>The total number of international calls that were abandoned on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_EMGNCY_ATTMP</td>
<td>The total number of Emergency call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_EMGNCY_FAIL</td>
<td>*The total number of Emergency call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_EMGNCY_CALL_SUCC</td>
<td>The total number of successful Emergency calls on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_EMGNCY_CALL_ABAND</td>
<td>The total number of Emergency calls that were abandoned on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_LOCAL_ATTMP</td>
<td>The total number of Local call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_LOCAL_FAIL</td>
<td>*The total number of Local call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_LOCAL_CALL_SUCC</td>
<td>The total number of successful Local calls on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_LOCAL_CALL_ABAND</td>
<td>The total number of Local calls that were abandoned on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_TOLL_FREE_ATTMP</td>
<td>The total number of Toll Free call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_TOLL_FREE_FAIL</td>
<td>*The total number of Toll Free call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_TOLL_FREE_CALL_SUCC</td>
<td>The total number of successful Toll Free calls on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_TOLL_FREE_CALL_ABAND</td>
<td>The total number of Toll Free calls that were abandoned on the reporting Call Agent.</td>
</tr>
<tr>
<td>Measurement</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>BCM_H323_ORIG_ATTEMPTS</td>
<td>The total number of originating H323 call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_H323_TERM_ATTEMPTS</td>
<td>The total number of terminating H323 call attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_H323_ORIG_FAILURES</td>
<td>The total number of originating H323 call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_H323_TERM_FAILURES</td>
<td>The total number of terminating H323 call attempts that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_H323_CALLS_SUCCESS</td>
<td>The total number of successful originating and terminating H323 calls on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_H323_CALLS_ABANDON</td>
<td>The total number of originating and terminating H323 calls that were abandoned on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_ISDN_H323_CALLS</td>
<td>The total number of successfully complete calls from an ISDN originator to an H323 terminator on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SS7_H323_CALLS</td>
<td>The total number of successfully complete calls from an SS7 originator to an H323 terminator on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_SIP_H323_CALLS</td>
<td>The total number of successfully complete calls from a SIP originator to an H323 terminator on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_MGCP_H323_CALLS</td>
<td>The total number of successfully complete calls from an MGCP originator to an H323 terminator on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_CAS_H323_CALLS</td>
<td>The total number of successfully complete calls from a CAS originator to an H323 terminator on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_H323_SIP_CALLS</td>
<td>The total number of successfully complete calls from an H323 originator to a SIP terminator on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_H323_ISDN_CALLS</td>
<td>The total number of successfully complete calls from an H323 originator to an ISDN terminator on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_H323_SS7_CALLS</td>
<td>The total number of successfully complete calls from an H323 originator to an SS7 terminator on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_H323_MGCP_CALLS</td>
<td>The total number of successfully complete calls from an H323 originator to an MGCP terminator on the reporting Call Agent.</td>
</tr>
</tbody>
</table>
### Table 19-6  Call Processing Measurements (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM_H323_CAS_CALLS</td>
<td>The total number of successfully complete calls from an H323 originator to a CAS terminator on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_H323_H323_CALLS</td>
<td>The total number of successfully complete calls from an H323 originator to an H323 terminator on the reporting Call Agent.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_AUTH_SUCC</td>
<td>Number of successful NAS Authentication Requests.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_AUTH_FAIL</td>
<td>Number of failed NAS Authentication Requests.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_OP_FAIL</td>
<td>Number of operation failures that occurred - typically a modem failure.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_ISP_PORT_LIMIT</td>
<td>Number of times a NAS call failed due to the port limit of a modem being exceeded.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_NO_MODEMS</td>
<td>Number of times a NAS call failed due to the unavailability of a modem.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_CLG_UNACC</td>
<td>Number of times a NAS call failed due to the calling number being blocked.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_CLD_UNACC</td>
<td>Number of times a NAS call failed due to the called number being blocked or is unknown.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_USER_REQUEST</td>
<td>Number of User Requests - Reason Code 801 - that are received in the DLCX messages.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_LOST_CARRIER</td>
<td>Number of Lost Carrier - Reason Code 802 - that are received in the DLCX messages.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_LOST_SERVICE</td>
<td>Number of Lost Service - Reason Code 803 - that are received in the DLCX messages.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_IDLE_TIMEOUT</td>
<td>Number of Idle Timeouts - Reason Code 804 - that are received in the DLCX messages.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_SESSION_TIMEOUT</td>
<td>Number of Session Timeouts - Reason Code 805 - that are received in the DLCX messages.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_ADMIN_RESET</td>
<td>Number of Admin Resets - Reason Code 806 - that are received in the DLCX messages.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_ADMIN_REBOOT</td>
<td>Number of Admin Reboots - Reason Code 807 - that are received in the DLCX messages.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_PORT_ERROR</td>
<td>Number of Port Errors - Reason Code 808 - that are received in the DLCX messages.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_NAS_ERROR</td>
<td>Number of NAS Errors - Reason Code 809 - that are received in the DLCX messages.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_NAS_REQUEST</td>
<td>Number of NAS Requests - Reason Code 810 - that are received in the DLCX messages.</td>
</tr>
</tbody>
</table>
Chapter 19      Traffic Measurements

Table 19-6  Call Processing Measurements (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM_TPM_NAS_NAS_REBOOT</td>
<td>Number of NAS Reboots - Reason Code 811 - that are received in the DLCX messages.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_PORT_UNNEEDED</td>
<td>Number of Port Unneededs - Reason Code 812 - that are received in the DLCX messages.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_PORT_PREEMPTED</td>
<td>Number of Port Preempteds - Reason Code 813 - that are received in the DLCX messages.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_PORT_SUSPENDED</td>
<td>Number of Port Suspendeds - Reason Code 814 - that are received in the DLCX messages.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_SERVICE_UNA VAIL</td>
<td>Number of Service Unavailables - Reason Code 815 - that are received in the DLCX messages.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_CALLBACK</td>
<td>Number of NAS Callbacks - Reason Code 816 - that are received in the DLCX messages.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_USER_ERROR</td>
<td>Number of User Errors - Reason Code 817 - that are received in the DLCX messages.</td>
</tr>
<tr>
<td>BCM_TPM_NAS_HOST_REQUEST</td>
<td>Number of Host Requests - Reason Code 818 - that are received in the DLCX messages.</td>
</tr>
</tbody>
</table>

H.323 Protocol Measurement Counters

Table 19-7 describes the H.323 protocol measurement counters.

Table 19-7  H.323 Protocol Measurement Counters

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>H323_SETUP_RECV</td>
<td>The total number of H323 SETUPs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_SETUP_SEND</td>
<td>The total number of H323 SETUPs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_SETUP_FAIL</td>
<td>The total number of H323 SETUPs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.</td>
</tr>
<tr>
<td>H323_CONNECT_RECV</td>
<td>The total number of H323 CONNECTs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_CONNECT_SEND</td>
<td>The total number of H323 CONNECTs transmitted by the reporting Call Agent.</td>
</tr>
</tbody>
</table>
**Table 19-7 H.323 Protocol Measurement Counters**

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>H323_CONNECT_FAIL</td>
<td>The total number of H323 CONNECT CONFIRMs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.</td>
</tr>
<tr>
<td>H323_ALERT_RECV</td>
<td>The total number of H323 ALERTs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_ALERT_SEND</td>
<td>The total number of H323 ALERTs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_ALERT_FAIL</td>
<td>The total number of H323 ALERTs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.</td>
</tr>
<tr>
<td>H323_IN_PROGRESS_RECV</td>
<td>The total number of H323 IN PROGRESSs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_IN_PROGRESS_SEND</td>
<td>The total number of H323 IN PROGRESSs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_IN_PROGRESS_FAIL</td>
<td>The total number of H323 IN PROGRESSs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.</td>
</tr>
<tr>
<td>H323_CALL_PROCEEDING_RECV</td>
<td>The total number of H323 CALL PROCEEDINGs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_CALL_PROCEEDING_SEND</td>
<td>The total number of H323 CALL PROCEEDINGs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_CALL_PROCEEDING_FAIL</td>
<td>The total number of H323 CALL PROCEEDINGs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.</td>
</tr>
<tr>
<td>H323_RELEASE_COMPLETE_RECV</td>
<td>The total number of H323 RELEASEs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_RELEASE_COMPLETE_SEND</td>
<td>The total number of H323 RELEASEs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_RELEASE_COMPLETE_FAIL</td>
<td>The total number of H323 RELEASEs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.</td>
</tr>
<tr>
<td>H323_REJECT_RECV</td>
<td>The total number of H323 REJECTs received by the reporting Call Agent.</td>
</tr>
</tbody>
</table>
## Table 19-7 H.323 Protocol Measurement Counters

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>H323_REJECT_SEND</td>
<td>The total number of H323 REJECTs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_REJECT_FAIL</td>
<td>The total number of H323 REJECTs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.</td>
</tr>
<tr>
<td>H323_INFORMATION_RECV</td>
<td>The total number of H323 INFOs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_INFORMATION_SEND</td>
<td>The total number of H323 INFOs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_INFORMATION_FAIL</td>
<td>The total number of H323 INFOs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.</td>
</tr>
<tr>
<td>H323_USER_INFO_RECV</td>
<td>The total number of H323 USER INFOs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_USER_INFO_SEND</td>
<td>The total number of H323 USER INFOs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_USER_INFO_FAIL</td>
<td>The total number of H323 USER INFOs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.</td>
</tr>
<tr>
<td>H323_FACILITY_RECV</td>
<td>The total number of H323 FACILITYs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_FACILITY_FAIL</td>
<td>The total number of H323 FACILITYs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.</td>
</tr>
<tr>
<td>H323_NOTIFY_RECV</td>
<td>The total number of H323 NOTIFYs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_NOTIFY_SEND</td>
<td>The total number of H323 NOTIFYs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_FACILITY_SEND</td>
<td>The total number of H323 FACILITYs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_NOTIFY_FAIL</td>
<td>The total number of H323 NOTIFYs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.</td>
</tr>
<tr>
<td>Measurement/Counter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>H323_PASSTHROU_RECV</td>
<td>The total number of H323 PASS THROUGHs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_PASSTHROU_SEND</td>
<td>The total number of H323 PASS THROUGHs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_PASSTHROU_FAIL</td>
<td>The total number of H323 PASS THROUGHs that failed. The failure is due to one of the following scenarios: unable to send due to full socket queue, unable to compose message due to invalid socket, or lack of available memory.</td>
</tr>
<tr>
<td>H323_GRQ_SEND</td>
<td>The total number of H323 GRQs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_GRQ_RECV</td>
<td>The total number of H323 GRQs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_GCF_SEND</td>
<td>The total number of H323 GCFs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_GCF_RECV</td>
<td>The total number of H323 GCFs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_GRJ_SEND</td>
<td>The total number of H323 GRJs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_GRJ_RECV</td>
<td>The total number of H323 GRJs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_RRQ_SEND</td>
<td>The total number of H323 RRQs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_RRQ_RECV</td>
<td>The total number of H323 RRQs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_RCF_SEND</td>
<td>The total number of H323 RCFs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_RCF_RECV</td>
<td>The total number of H323 RCFs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_RRJ_SEND</td>
<td>The total number of H323 RRJs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_RRJ_RECV</td>
<td>The total number of H323 RRJs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_ARQ_SEND</td>
<td>The total number of H323 ARQs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_ARQ_RECV</td>
<td>The total number of H323 ARQs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_ACF_SEND</td>
<td>The total number of H323 ACFs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_ACF_RECV</td>
<td>The total number of H323 ACFs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>Measurement/Counter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>H323_ARJ_SEND</td>
<td>The total number of H323 ARJs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_ARJ_RECV</td>
<td>The total number of H323 ARJs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_BRQ_SEND</td>
<td>The total number of H323 BRQs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_BRQ_RECV</td>
<td>The total number of H323 BRQs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_BCF_SEND</td>
<td>The total number of H323 BCFs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_BCF_RECV</td>
<td>The total number of H323 BCFs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_BRJ_SEND</td>
<td>The total number of H323 BRJs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_BRJ_RECV</td>
<td>The total number of H323 BRJs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_DRQ_SEND</td>
<td>The total number of H323 DRQs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_DRQ_RECV</td>
<td>The total number of H323 DRQs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_DCF_SEND</td>
<td>The total number of H323 DCFs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_DCF_RECV</td>
<td>The total number of H323 DCFs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_DRJ_SEND</td>
<td>The total number of H323 DRJs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_DRJ_RECV</td>
<td>The total number of H323 DRJs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_URQ_SEND</td>
<td>The total number of H323 URQs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_URQ_RECV</td>
<td>The total number of H323 URQs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_UCF_SEND</td>
<td>The total number of H323 UCFs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_UCF_RECV</td>
<td>The total number of H323 UCFs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_URJ_SEND</td>
<td>The total number of H323 URJs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_URJ_RECV</td>
<td>The total number of H323 URJs received by the reporting Call Agent.</td>
</tr>
</tbody>
</table>
### Table 19-7  H.323 Protocol Measurement Counters

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description (*=rapid count can mean a potential problem in the system)</th>
</tr>
</thead>
<tbody>
<tr>
<td>H323_RIP_SEND</td>
<td>The total number of H323 RIPs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_RIP_RECV</td>
<td>The total number of H323 RIPs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_RAI_SEND</td>
<td>The total number of H323 RAIs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_RAI_RECV</td>
<td>The total number of H323 RAIs received by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_RAC_SEND</td>
<td>The total number of H323 RACs transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>H323_RAC_RECV</td>
<td>The total number of H323 RACs received by the reporting Call Agent.</td>
</tr>
</tbody>
</table>

### SIP-T Adapter Measurement Counters

Table 19-8 describes the SIP-T Adapter (SIA) measurement counters.

### Table 19-8  SIP-T Adapter (SIA) Measurement Counters

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description (*=rapid count can mean a potential problem in the system)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_TOTAL_INCOMING_MSG</td>
<td>The total number of incoming SIP message attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_TOTAL_SUCCESS_INCOMING_MSG</td>
<td>The total number of successfully received incoming SIP messages on the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_TOTAL_OUTGOING_MSG</td>
<td>The total number of outgoing SIP message transmit attempts on the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_TOTAL_SUCCESS_OUTGOING_MSG</td>
<td>The total number of successfully transmitted outgoing SIP messages on the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_REQ_RETRAN_RCVD</td>
<td>*The total number of SIP request retransmission messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_REQ_RETRAN_SENT</td>
<td>*The total number of SIP request retransmission messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_RSP_RETRAN_RCVD</td>
<td>*The total number of SIP response retransmission messages received by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>Measurement/Counter</td>
<td>Description (*=rapid count can mean a potential problem in the system)</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>SIP_RSP_RETRAN_SENT</td>
<td>*The total number of SIP response retransmission messages transmitted by the reporting Call Agent or Feature Server.</td>
</tr>
<tr>
<td>SIP_T1_TIMER_EXPIRED</td>
<td>*The total number of T1 Timer expirations that occurred during the current collection interval on the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_T2_TIMER_REACHED</td>
<td>*The total number of T2 Timer expirations that occurred during the current collection interval on the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_INVITE_RECEIVED</td>
<td>The total number of INVITE messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_INVITE_SENT</td>
<td>The total number of INVITE messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_CANCEL_RECEIVED</td>
<td>The total number of CANCEL messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_CANCEL_SENT</td>
<td>The total number of CANCEL messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_BYE_RECEIVED</td>
<td>The total number of BYE messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_BYE_SENT</td>
<td>The total number of BYE messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_ACK_RECEIVED</td>
<td>The total number of ACK messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_ACK_SENT</td>
<td>The total number of ACK messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_OPTIONS_RECEIVED</td>
<td>The total number of OPTION messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_OPTIONS_SENT</td>
<td>The total number of OPTION messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_REGISTER_RECEIVED</td>
<td>The total number of REGISTER messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_REGISTER_SENT</td>
<td>The total number of REGISTER messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_INFO_RECEIVED</td>
<td>The total number of INFO messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_INFO_SENT</td>
<td>The total number of INFO messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_NOTIFY_RECEIVED</td>
<td>The total number of NOTIFY messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_NOTIFY_SENT</td>
<td>The total number of NOTIFY messages transmitted by the reporting Call Agent.</td>
</tr>
</tbody>
</table>
## Table 19-8  SIP-T Adapter (SIA) Measurement Counters (continued)

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_100_RECEIVED</td>
<td>The total number of 100 (trying) messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_100_SENT</td>
<td>The total number of 100 (trying) messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_18x_RECEIVED</td>
<td>The total number of 18x (informational) messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_18x_SENT</td>
<td>The total number of 18x (informational) messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_200_RECEIVED</td>
<td>The total number of 200 (success) messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_200_SENT</td>
<td>The total number of 200 (success) messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_3xx_RECEIVED</td>
<td>The total number of 3xx (redirection) messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_3xx_SENT</td>
<td>The total number of 3xx (redirection) messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_4xx_RECEIVED</td>
<td>*The total number of 4xx (request failures) messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_4xx_SENT</td>
<td>*The total number of 4xx (request failures) messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_5xx_RECEIVED</td>
<td>*The total number of 5xx (server failures) messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_5xx_SENT</td>
<td>*The total number of 5xx (server failures) messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_6xx_RECEIVED</td>
<td>*The total number of 6xx (global failures) messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_6xx_SENT</td>
<td>*The total number of 6xx (global failures) messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_7xx_RECEIVED</td>
<td>The total number of 7xx (reserved) messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_7xx_SENT</td>
<td>The total number of 7xx (reserved) messages transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_PROV_RSP_RETRAN_RCVD</td>
<td>The number of SIP provisioning response retransmission messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_PROV_RSP_RETRAN_SENT</td>
<td>The number of SIP provisioning response retransmission messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_PRACK_RECEIVED</td>
<td>The number of SIP PRACK messages the reporting Call Agent or Feature Server received.</td>
</tr>
</tbody>
</table>
Table 19-8  SIP-T Adapter (SIA) Measurement Counters (continued)

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_PRACK_SENT</td>
<td>The number of SIP PRACK messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_SUBSCRIBE_RECEIVED</td>
<td>The number of SIP SUBSCRIBE messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_SUBSCRIBE_SENT</td>
<td>The number of SIP SUBSCRIBE messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIPREFER_RECEIVED</td>
<td>The number of SIP REFER messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIPREFER_SENT</td>
<td>The number of SIP REFER messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIPREFER_REPLACES_RECEIVED</td>
<td>The number of SIP REFER REPLACES messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_INVITE_REPLACES_SENT</td>
<td>The number of SIP INVITE REPLACES messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_INVITE_REPLACES_RECEIVED</td>
<td>The number of SIP INVITE REPLACES messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_REL100_RECEIVED</td>
<td>The number of REL100 class (TRYING) messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_REL100_SENT</td>
<td>The number of REL100 class (TRYING) messages the reporting Call Agent or Feature Server sent.</td>
</tr>
<tr>
<td>SIP_UNSUPPORTED_RECEIVED</td>
<td>The number of unsupported SIP messages the reporting Call Agent or Feature Server received.</td>
</tr>
<tr>
<td>SIP_OG_CALL_INIT</td>
<td>The number of outgoing SIP call initializations on the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_OG_CALL_SUCCEEDED</td>
<td>The number of successful outgoing SIP calls on the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_OG_CALL_FAILED</td>
<td>*The number of outgoing SIP calls that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_IC_CALL_INIT</td>
<td>The number of incoming SIP call initializations on the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_IC_CALL_SUCCEEDED</td>
<td>The number of successful incoming SIP calls on the reporting Call Agent.</td>
</tr>
<tr>
<td>SIP_IC_CALL_FAILED</td>
<td>*The number of incoming SIP calls that failed on the reporting Call Agent.</td>
</tr>
<tr>
<td>TOTAL_SUCCESS_CALL</td>
<td>The total number of successfully completed SIP calls on the reporting Call Agent.</td>
</tr>
</tbody>
</table>
**Table 19-8  SIP-T Adapter (SIA) Measurement Counters (continued)**

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description (*=rapid count can mean a potential problem in the system)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOTAL_UNSUCCESS_CALL</td>
<td>*The total number of unsuccessfully completed SIP calls on the reporting Call Agent.</td>
</tr>
<tr>
<td>TOTAL_UNSUCCESS_OUTGOING_MSG</td>
<td>*The total number of outgoing SIP message attempts that were not successfully transmitted by the reporting Call Agent.</td>
</tr>
<tr>
<td>TOTAL_UNSUCCESS_INCOMING_MSG</td>
<td>*The total number of incoming SIP message attempts that were not successfully received by the reporting Call Agent.</td>
</tr>
</tbody>
</table>

**ISDN Measurements**

Table 19-9 describes the ISDN measurement counters.

**Table 19-9  ISDN Measurement Counters**

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description (*=rapid count can mean a potential problem in the system)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISDN_SETUP_TX</td>
<td>The number of ISDN SETUP messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_SETUP_RX</td>
<td>The number of ISDN SETUP messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_SETUP_ACK_TX</td>
<td>The number of ISDN SETUP ACK messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_SETUP_ACK_RX</td>
<td>The number of ISDN SETUP ACK messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_CALL_PROCEED_TX</td>
<td>The number of ISDN CALL PROCEED messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_CALL_PROCEED_RX</td>
<td>The number of ISDN CALL PROCEED messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_ALERTING_TX</td>
<td>The number of ISDN ALERTING messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_ALERTING_RX</td>
<td>The number of ISDN ALERTING messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_PROGRESS_TX</td>
<td>The number of ISDN PROGRESS messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_PROGRESS_RX</td>
<td>The number of ISDN PROGRESS messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_CONNECT_TX</td>
<td>The number of ISDN CONNECT messages sent from the reporting Call Agent.</td>
</tr>
</tbody>
</table>
### Table 19-9 ISDN Measurement Counters (continued)

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISDN_CONNECT_RX</td>
<td>The number of ISDN CONNECT messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_CONNECT_ACK_TX</td>
<td>The number of ISDN CONNECT ACK messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_CONNECT_ACK_RX</td>
<td>The number of ISDN CONNECT ACK messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_DISCONNECT_TX</td>
<td>The number of ISDN DISCONNECT messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_DISCONNECT_RX</td>
<td>The number of ISDN DISCONNECT messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_RELEASE_TX</td>
<td>The number of ISDN RELEASE messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_RELEASE_RX</td>
<td>The number of ISDN RELEASE messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_RELEASE_COMPLETE_TX</td>
<td>The number of ISDN RELEASE COMPLETE messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_RELEASE_COMPLETE_RX</td>
<td>The number of ISDN RELEASE COMPLETE messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_RESTART_TX</td>
<td></td>
</tr>
<tr>
<td>ISDN_RESTART_RX</td>
<td></td>
</tr>
<tr>
<td>ISDN_RESTART_ACK_TX</td>
<td>*The number of ISDN RESTART ACK messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_RESTART_ACK_RX</td>
<td>*The number of ISDN RESTART ACK messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_INFORMATION_TX</td>
<td>The number of ISDN INFORMATION messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_INFORMATION_RX</td>
<td>The number of ISDN INFORMATION messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_NOTIFY_TX</td>
<td>The number of ISDN NOTIFY messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_NOTIFY_RX</td>
<td>The number of ISDN NOTIFY messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_STATUS_TX</td>
<td>The number of ISDN STATUS messages sent from the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_STATUS_RX</td>
<td>The number of ISDN STATUS messages received by the reporting Call Agent.</td>
</tr>
<tr>
<td>ISDN_STATUS_ENQUIRY_TX</td>
<td>The number of ISDN STATUS ENQUIRY messages sent from the reporting Call Agent.</td>
</tr>
</tbody>
</table>
### Billing Measurement Counters

Table 19-10 describes the billing measurement counters.

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description (*=rapid count can mean a potential problem in the system)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALLTYPE_TEST_CALL</td>
<td>The number of Test Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_INTL</td>
<td>The number of International Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_LOCAL</td>
<td>The number of Local Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_TOLL</td>
<td>The number of Toll Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_INTERLATA</td>
<td>The number of Interlata Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_TANDEM</td>
<td>The number of Tandem Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_EMG</td>
<td>The number of Emergency 911 Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_NON_EMG</td>
<td>The number of non-emergency 311 Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_DA</td>
<td>The number of Directory Assistance Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_DA_TOLL</td>
<td>The number of Directory Assistance Toll Call billing records created in the reporting Call Agent.</td>
</tr>
</tbody>
</table>
### Table 19-10 Billing Measurement Counters (continued)

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALLTYPE_REPAIR</td>
<td>The number of Repair Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_RELAY</td>
<td>The number of Relay Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_BUSINESS</td>
<td>The number of Business Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_TOLL_FREE</td>
<td>The number of Toll Free Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_900</td>
<td>The number of 900 Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_PCS</td>
<td>The number of PCS Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_VACANT</td>
<td>The number of Vacant Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_INVALID</td>
<td>The number of Invalid Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_500</td>
<td>The number of 500 Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_700</td>
<td>The number of 700 Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_976</td>
<td>The number of 976 Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_NONE</td>
<td>The number of billing records of unknown type created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_LRN</td>
<td>The number of LRN Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_EXTENSION</td>
<td>The number of Extension Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_CUT_THRU</td>
<td>The number of Cut Thru Call billing records created in the reporting Call Agent.</td>
</tr>
<tr>
<td>CALLTYPE_OPERATOR</td>
<td>The number call detail blocks of type cut operator created by the reporting Element Management System.</td>
</tr>
<tr>
<td>CALLTYPE_CARRIER_OPERATOR</td>
<td>The number call detail blocks of type carrier operator created by the reporting Element Management System.</td>
</tr>
<tr>
<td>CALLTYPE_OPERATOR_ASSISTED</td>
<td>The number call detail blocks of type operator assisted created by the reporting Element Management System.</td>
</tr>
<tr>
<td>CALLTYPE_BLV</td>
<td>The number call detail blocks of type busy line verification created by the reporting Element Management System.</td>
</tr>
</tbody>
</table>
### Table 19-10 Billing Measurement Counters (continued)

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALLTYPE_SPEED_DIAL</td>
<td>The number call detail blocks of type speed dial created by the reporting Element Management System.</td>
</tr>
<tr>
<td>CALLTYPE_NATIONAL</td>
<td>The number call detail blocks of type national (NANP) created by the reporting Element Management System.</td>
</tr>
<tr>
<td>CALLTYPE_TW</td>
<td>The number call detail blocks of type time and weather created by the reporting Element Management System.</td>
</tr>
<tr>
<td>CALLTYPE_INFO</td>
<td>The number call detail blocks of type information (i.e. 976 calls) created by the reporting Element Management System.</td>
</tr>
<tr>
<td>CALLTYPE_PREMIUM</td>
<td>The number call detail blocks of type premium (i.e. 900 calls) created by the reporting Element Management System.</td>
</tr>
<tr>
<td>CALLTYPE_ATTENDANT</td>
<td>The number call detail blocks of type attendant created by the reporting Element Management System.</td>
</tr>
<tr>
<td>CALLTYPE_NAS</td>
<td>The number call detail blocks of type NAS created by the reporting Element Management System.</td>
</tr>
<tr>
<td>CALLTYPE_POLICE</td>
<td>The number call detail blocks of type police created by the reporting Element Management System.</td>
</tr>
<tr>
<td>CALLTYPE_FIRE</td>
<td>The number call detail blocks of type fire created by the reporting Element Management System.</td>
</tr>
<tr>
<td>CALLTYPE_AMBULANCE</td>
<td>The number call detail blocks of type ambulance created by the reporting Element Management System.</td>
</tr>
<tr>
<td>CALLTYPE_TIME</td>
<td>The number call detail blocks of type time created by the reporting Element Management System.</td>
</tr>
<tr>
<td>CALLTYPE_WEATHER</td>
<td>The number call detail blocks of type weather created by the reporting Element Management System.</td>
</tr>
<tr>
<td>CALLTYPE_TRAFFIC</td>
<td>The number call detail blocks of type traffic created by the reporting Element Management System.</td>
</tr>
<tr>
<td>BILLING_EM_ACKED</td>
<td>The number of event messages acknowledged by the Record Keeping System.</td>
</tr>
<tr>
<td>BILLING_EM_LOGGED</td>
<td>The number of event messages written to disk.</td>
</tr>
<tr>
<td>BILLING_EM_RETRANS</td>
<td>The number of event messages that were retransmitted due to a lack of acknowledgment by the Record Keeping System.</td>
</tr>
</tbody>
</table>

### SNMP Measurements

Table 19-11 describes the SNMP measurement counters.
List of Traffic Measurements (Counters)

Table 19-11 SNMP Measurement Counters

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP_TRAP_TX</td>
<td>The total number of SNMP TRAPs generated by the report Element Management System.</td>
</tr>
<tr>
<td>SNMP_SET_RX</td>
<td>The total number of SNMP SET command requests received by the reporting Element Management System.</td>
</tr>
<tr>
<td>SNMP_SET_TX</td>
<td>The total number of SNMP SET command responses transmitted by the reporting Element Management System.</td>
</tr>
<tr>
<td>SNMP_GET_RX</td>
<td>The total number of SNMP GET command requests received by the reporting Element Management System.</td>
</tr>
<tr>
<td>SNMP_GET_TX</td>
<td>The total number of SNMP GET command responses transmitted by the reporting Element Management System.</td>
</tr>
<tr>
<td>SNMP_GET_NEXT_RX</td>
<td>The total number of SNMP GETNEXT command requests received by the reporting Element Management System.</td>
</tr>
<tr>
<td>SNMP_GET_NEXT_T</td>
<td>The total number of SNMP GETNEXT command responses transmitted by the reporting Element Management System.</td>
</tr>
</tbody>
</table>

Trunk Group Usage Measurement Counters

Table 19-12 describes the TG usage measurement counters.

Table 19-12 Trunk Group Usage Measurements

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRK_GRP_TYPE</td>
<td>The signaling type of the reporting trunk group.</td>
</tr>
<tr>
<td>TRK_GRP_ID</td>
<td>The identification number of the reporting trunk group.</td>
</tr>
<tr>
<td>INCOMING_CALL_ATTMP</td>
<td>The number of times the system recognizes an incoming seizure for any trunk within the reporting group.</td>
</tr>
<tr>
<td>OUTGOING_CALL_ATTMP</td>
<td>The number of times the system tries to access any trunk for outbound calls within the reporting trunk group.</td>
</tr>
<tr>
<td>OUTBOUND_CALL_FAIL</td>
<td>The number of times the system tries to access a any trunk within the reporting trunk group and is unsuccessful.</td>
</tr>
<tr>
<td>NUM_OF_OVERFLOW</td>
<td>The number of outgoing trunk call attempt failures due all trunks within the reporting trunk group being unavailable.</td>
</tr>
<tr>
<td>NUM_OF_TRUNK</td>
<td>The total number of trunks within the reporting trunk group.</td>
</tr>
<tr>
<td>INCOMING_BSY_TRK</td>
<td>Summation of the number of trunk circuits within the reporting trunk group marked as BUSY with originating calls taken every 100 seconds during the interval.</td>
</tr>
<tr>
<td>OUTGOING_BSY_TRK</td>
<td>Summation of the number of trunk circuits within the reporting trunk group marked as BUSY with terminating calls taken every 100 seconds during the interval.</td>
</tr>
</tbody>
</table>
**Table 19-12 Trunk Group Usage Measurements**

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUM_OF_OOS_TRK</td>
<td>*The total number of transitions to the LOCALLY BLOCKED state for all trunk circuits within the reporting trunk group.</td>
</tr>
<tr>
<td>INCOMING_USAGE</td>
<td>Summation of the number of trunk circuits within the reporting trunk group marked as BUSY with originating calls taken every 100 seconds during the interval.</td>
</tr>
<tr>
<td>OUTGOING_USAGE</td>
<td>Summation of the number of trunk circuits within the reporting trunk group marked as BUSY with terminating calls taken every 100 seconds during the interval.</td>
</tr>
<tr>
<td>TOTAL_USAGE</td>
<td>Summation of the incoming-busy-trunk and outgoing-busy-trunk counters for the reporting trunk group.</td>
</tr>
<tr>
<td>AVERAGE_USAGE</td>
<td>The total-usage counter divided by the number of trunks in the reporting trunk group.</td>
</tr>
</tbody>
</table>

**Announcement Measurement Counters**

Table 19-13 describes the announcement measurement counters.

**Table 19-13 Announcement Measurement Counters**

<table>
<thead>
<tr>
<th>Measurement/Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANM_TPM_CKT_UNAVAIL</td>
<td>*The number of calls resulting in the playing of the circuit unavailable announcement.</td>
</tr>
<tr>
<td>ANM_TPM_CALL_REJECTED</td>
<td>*The number of calls resulting in the playing of the call rejected announcement.</td>
</tr>
<tr>
<td>ANM_TPM_ADDR_INCOMPLETE</td>
<td>*The number of calls resulting in the playing of the address incomplete announcement.</td>
</tr>
<tr>
<td>ANM_TPM_FAC_REJECTED</td>
<td>*The number of calls resulting in the playing of the facility rejected announcement.</td>
</tr>
<tr>
<td>ANM_TPM_PRE_0_1_ABSENT</td>
<td>The number of calls resulting in the playing of the prefix of 0 or 1 absent announcement.</td>
</tr>
<tr>
<td>ANM_TPM_PRE_0_1_PRESENT</td>
<td>The number of calls resulting in the playing of the prefix 0 or 1 present announcement.</td>
</tr>
<tr>
<td>ANM_TPM_HNPA_ABSENT</td>
<td>The number of calls resulting in the playing of the HNPA area code announcement.</td>
</tr>
<tr>
<td>ANM_TPM_NO_ROUTE_DEST</td>
<td>*The number of calls resulting in the playing of the no route to destination announcement.</td>
</tr>
<tr>
<td>ANM_TPM_UNALLOCATED_NUM</td>
<td>The number of calls resulting in the playing of the unallocated number announcement.</td>
</tr>
<tr>
<td>Measurement/Counter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ANM_TPM_NUM_CHANGED</td>
<td>The number of calls resulting in the playing of the number changed announcement.</td>
</tr>
<tr>
<td>ANM_TPM_DEST_OUTOFORDER</td>
<td>The number of calls resulting in the playing of the destination out of order announcement.</td>
</tr>
<tr>
<td>ANM_TPM_TEMP_DISCONNECT</td>
<td>The number of calls resulting in the playing of the temporarily disconnected announcement.</td>
</tr>
<tr>
<td>ANM_TPM_FEAT_NOT_SUBS</td>
<td>The number of calls resulting in the playing of the feature not subscribed to announcement.</td>
</tr>
<tr>
<td>ANM_TPM_AUTHCODE_INVALID</td>
<td>The number of calls resulting in the playing of the authorization code invalid announcement.</td>
</tr>
<tr>
<td>ANM_TPM_NO_RTE_TRANSITNW</td>
<td>*The number of calls resulting in the playing of the no route to specified network announcement.</td>
</tr>
<tr>
<td>ANM_TPM_CAUSE_UNKNOWN</td>
<td>The number of calls resulting in the playing of the cause unknown announcement.</td>
</tr>
</tbody>
</table>
Audit Database and Table Name

This chapter describes how to audit databases and table names. The commands described in this chapter allow a user to audit either the complete database or entries in every table that can be provisioned in both the Oracle database and shared memory.

**Note**
All audit commands are time intensive. Completion time depends upon the number of entries in the table or database.

## Audit Database

The audit database command allows users to audit table entries two ways using the **type** and/or the **platform state** token. Users can either audit every entry in every table that can be provisioned, by omitting all tokens, which returns a listing of every entry in every table. Or, the audit can be restricted using the **type** and **platform state** tokens.

**Note**
If a type parameter is not specified, the type default is **full**. If a platform-state is not specified, the default is **active**.

**Step 1**
Use one of the following examples to audit the entire database, or restrict the audit using tokens:

```plaintext
audit database;
audit database type=row-count;
audit database platform-state=ems;
```

## Table Name

The audit table name command audits only the entries in a particular table `<table-name>` (where table-name is any provisionable table). The audit is made more specific by specifying tokens and values from the particular table being audited that narrow the search. For example, if a user types `audit service`, that audits the entire service table. If a user types `audit service id=123`, that audits only the service entry with the ID of 123. The audit is also made more specific by specifying a type and/or platform state from the particular table that narrows the search.
Table Name

Chapter 20      Audit Database and Table Name

Step 1
Use one of the following examples to audit the entire database, or restrict the audit by using the type token:

audit trunk type=row-count;
audit trunk platform-state=active; tgn-id=42;
audit subscriber id=jer%;

Note  The last example shows how to use the percent sign (%) to specify a search range. This example returns any subscriber entries that have an ID field beginning with jer.
Database Usage

The Database Usage (db-usage) command returns and modifies the maximum number of records allowed, as well as the number of licensed and current database records. Records can be shown and changed. Records cannot be deleted.

The current number of records field is updated by the EMS in real time. The db-usage command also uses the Database Threshold (db-thresholds) table, which contains default alarm threshold parameters that are preprovisioned during installation. Parameters can be changed and shown. The default threshold parameters are:

- 80 percent minor
- 85 percent major
- 90 percent critical

Note
Do not use a hyphen (-) in the actual name of a table when using this command. Use the underscore (_). For example, dial_plan is correct; dial-plan is not correct.

Show

This section describes the show db-usage command.

Step 1
Use the following command example to show db-usage statistics:

```
show db-usage table-name=dial-plan;
```

Change

This section describes the change db-usage command.

Step 1
Use the following command example to change db-usage tokens and values.

```
change db-usage table-name=dial-plan; minor-threshold=70; major-threshold=80; critical-threshold=95;
```
Transactions

This chapter describes the commands and tables for viewing and manipulating transactions.

Transaction Queue

The transaction-queue command allows users to view and delete entries in a transaction queue, if any exist. The Transaction Queue table tracks updates into the database, as well as into the shared memory of the Call Agent and Feature Servers. Entries should never remain in the transaction queue for more than a few seconds, unless an Element Management System (EMS), Call Agent, or Feature Server is in an error state. In the case of an error state, the transaction queue continues to store entries for later updates. Transaction queue entries can be deleted but not changed.

Show

This section describes the transaction-queue show command.

Step 1 Use the following command example to show any entries in a transaction queue:

```
show transaction-queue target=CA146
```

Delete

This section describes the transaction-queue delete command.

Step 1 Use the following command example to delete any entries in a transaction queue.

```
delete transaction-queue target=CA146
```

Caution

The `delete transaction-queue` command causes a database inconsistency. Call the Cisco Systems Technical Assistance Center to determine usage necessity.
Queue Throttle

The queue-throttle command allows provisioning commands to be throttled by changing the percentage of the maximum download capacity used for transaction queuing. It constrains transactions on a particular Call Agent, Feature Server, or EMS during provisioning. Queue throttle entries can be shown but not changed or deleted.

Use the following command example to show any queue throttle entries:

```
show queue-throttle
```
History

The history command returns a list of all executed commands. A list of all executed commands can be sent to a file (report history) or displayed on the screen (show history).

Show

This section describes the history show command. Results of this command are sent to the terminal screen. Using this command without any tokens returns all entries.

Step 1

Use the following command example to show all history entries:

show history;

Report

This section describes the history report command. Results of this command are sent to a report file. Using this command without any tokens returns all entries.

Step 1

Use the following command example to report all history entries:

report history;

Step 2

Using the Cisco BTS 10200 Softswitch http:// server in an external browser (Netscape, Internet Explorer, and so forth), perform the following steps to retrieve the history report file:

a. Enter the http:// server name.
   
   http://<your bts domain name>:10200> <enter>

b. Once on the main page, click the reports link.
   
   A set of directories appears.

c. Select the Command History report by clicking history.html.
   
   The history log appears.
Call Trace Summary

The Call Trace Summary command reports the information gathered when a customer activates a trace by pressing *57 on the telephone. This command logs information pertaining only to the most recently received call. Report is the only command type. Using the command without any tokens returns all entries in the table.

Use the following command example to report call trace information:

```
report call-trace-summary
```

**Note**
Table information is logged from the switch. If the system cannot decipher the information from the switch, it returns the value UNKNOWN in the applicable field.

The report appears on the screen. No HTML report is generated.
Command Scheduler

The Command Scheduler allows you to schedule a command to execute daily, weekly, or monthly at a specific time. Once a command is scheduled, the Scheduler allows you to remove a command from the schedule. Regardless of whether the command previously executed, the command can be removed at any time. If the command is scheduled to recur and is currently executing within the Element Management System (EMS), the command completes in a normal fashion but is removed from the list from that point forward.

It is often necessary to schedule commands to occur during periods of least system activity. Using the start-time and recurrence command tokens, you can schedule commands at any time and at any frequency. The recurrence token schedules a command daily, weekly, or monthly. Scheduling a command without the recurrence token causes the Command Scheduler to execute the command only once.

The characteristics of a scheduled command are read once at execution time. During execution, the characteristics can be changed but do not affect the command that is running.

Show

This section describes the scheduled-command show command.

**Step 1**

Use the following command example to show a particular scheduled command:

```
show scheduled-command id=1234;
```

_A Note_ A command must be added before it can be shown.

Add

This section describes the scheduled-command add command.

**Step 1**

Use the following command example to add a scheduled command:

```
add scheduled-command start-time=2001-10-01 12:22:22; noun=database; verb=audit;
```
Change

This section describes the scheduled-command change command.

**Step 1** Use the following command example to change a scheduled command:

```plaintext
change scheduled-command id=1234; start-time=2001-10-02 20:00:00;
```

Delete

This section describes the scheduled-command delete command.

**Step 1** Use the following command example to delete a scheduled command:

```plaintext
delete scheduled-command id=1234;
```
This chapter describes how to back up and restore the Cisco BTS 10200 Softswitch. Cisco Systems recommends backing up the Cisco BTS 10200 Softswitch on a daily basis. In these procedures, the following Cisco BTS 10200 Softswitch components are on the same machine (host), and are backed up together in a single process:

- CA—Call Agent
- FSPTC—POTS, Tandem and Centrex Feature Server
- FSAIN—AIN Feature Server

Refer to the Cisco BTS 10200 Softswitch Disaster Recovery Procedures Release 3.5 feature module for Element Management System (EMS) backup information. EMS backup and recovery procedures are not covered in this document.

Access to the Cisco BTS 10200 Softswitch is by Secure Shell (SSH).

**Back Up the Cisco BTS 10200 Softswitch**

This section describes how to back up the Cisco BTS 10200 Softswitch.

**Remote Network File Server Preparation**

To identify the remote network file server (NFS) for backup, perform the following steps:

**Step 1**
Confirm that you have a connection suitable for transferring files via FTP between the Cisco BTS 10200 Softswitch and a remote NFS that is connected to a corporate LAN and backed up daily. The NFS must be pingable and mountable from the Cisco BTS 10200 Softswitch.

**Step 2**
On the remote NFS, create the subdirectory where the backup file will be stored.

```bash
mkdir -p /.../.../BTS_Backups/BTS_Backup_mmdd
```
## Log In to the Standby Cisco BTS 10200 Softswitch

To log in to the standby (secondary or side B) Cisco BTS 10200 Softswitch, perform the following steps.

### Note
The Call Agent and the Feature Server must be running on the same host.

### Step 1
Ensure that your local PC or workstation has connectivity via TCP/IP to communicate with the standby Cisco BTS 10200 Softswitch unit that you are backing up.

### Step 2
Open a UNIX shell (or, in Windows, choose **Start>Run>Command Prompt**) or XTerm window.

### Step 3
At the UNIX shell prompt, enter `ssh`, `root`, and the host name or domain name of the standby Cisco BTS 10200 Softswitch.

### Note
It is best to use the standby (and not the active) Cisco BTS 10200 Softswitch machine, because the file transfer in this procedure can take up to 10 minutes.

```
ssh -l root <host-name>
```

The password prompt appears.

### Step 4
Enter the root password.

```
<root password>
```

A `<hostname>` # prompt appears, where `<hostname>` is the machine name for the active Cisco BTS 10200 Softswitch.

## Terminate All Applications on the Standby Cisco BTS 10200 Softswitch

To terminate all applications on the standby Cisco BTS 10200 Softswitch, perform the following steps:

### Step 1
Log in as `root`.

### Step 2
Bring up the Omni Termhandler utility.

```
<hostname> cd /opt/omni/bin
<hostname> termhandler -node a7n1
```

### Step 3
Deactivate any SS7 links on CA/FS side B.

```
OMNI [date] #1:deact-slk:slk=<link on standby Cisco BTS 10200 Softswitch >;
```

The prompt “Continue Y/N” appears.
Enter Y to continue.
Repeat Step 3 for each active link

**Step 4** Confirm the link status.

```
OMNI [date] #2:display-slk;
```

The prompt “Continue Y/N” appears.
Enter Y to continue.
Verify that the state of each link on the standby Cisco BTS 10200 Softswitch is INACTIVE.

**Step 5** Exit the Omni Termhandler utility.

```
OMNI[date]#3:quit
```

**Step 6** Terminate all applications on the standby Cisco BTS 10200 Softswitch.

```
<hostname>#$ platform stop all
```

## Run a Backup of the Cisco BTS 10200 Softswitch

To run a backup of the Cisco BTS 10200 Softswitch, perform the following steps:

**Step 1** At the prompt of the standby Cisco BTS 10200 Softswitch machine, navigate to the utils directory.

```
cd /opt/ems/utils
```

**Step 2** Run the backup.

```
./dataBackRes -b
```

**Note** In this command, -b means the backup process.

**Note** Depending upon the shared data file size, this process can take up to 10 minutes.

**Step 3** Once the data backup is finished and the prompt is displayed, navigate to the backup directory.

```
cd /opt/ems/backup
```

**Step 4** List the files in the backup directory. The following command lists the files in reverse order by creation date.

```
ls -lrt
```

**Step 5** Check that the proper files (as listed in Table 26-1) are present. Be sure to check that the filenames include the correct date stamp in the format *mmddhhmm*, where hh=00 to 24.

The types of backup files for the Cisco BTS 10200 Softswitch are listed in Table 26-1.
Back Up the Cisco BTS 10200 Softswitch

Step 6  Use the following command to compute a checksum on each of the selected files. These checksum values will be used later for comparison to checksums taken on the files after transfer to the remote NFS is complete.

$ cksum <file name>

Step 7  Record and save these checksum values in any convenient manner.

### Activate All Applications on the Standby Cisco BTS 10200 Softswitch

To activate all applications on the standby Cisco BTS 10200 Softswitch, perform the following steps:

**Step 1**  Activate the applications.

```
<hostname>$ platform start
```

**Step 2**  Bring up Omni Termhandler utility.

```
<hostname>$ cd /opt/omni/bin
<hostname>$ termhandler -node a7n1
```

**Step 3**  Activate SS7 links on the standby Cisco BTS 10200 Softswitch.

```
OMNI [date] #1:actv-slk:slk=< link on standby Cisco BTS 10200 Softswitch >;
```

The prompt “Continue Y/N” appears.

Enter Y to continue.

Repeat Step 3 for each inactive link.

**Step 4**  Confirm the link status.

```
OMNI [date] #2:display-slk;
```

Enter Y to continue.

Verify that the state of each link is active.

**Step 5**  Exit the Omni Termhandler utility.
Use FTP to Back Up Files to a Remote NFS

To use the FTP facility to back up the files to a remote Network File Server (NFS), perform the following steps.

**Note**
Depending upon the security policy of the remote NFS, you may need to use secure FTP (SFTP) to execute these steps.

**Step 1**
Log in to the remote NFS by entering your username and password for that system.

**Step 2**
At the prompt, establish an FTP session with the remote server.

\`ftp <remote server name>\`

**Step 3**
When prompted, enter your username and password for the remote NFS.

The FTP prompt appears.

**Step 4**
Enter `bin` to enable binary transfer.

**Note**
If you are using SFTP, skip to Step 4.

**Step 5**
On the remote NFS, navigate to the subdirectory where the backup file will be stored.

\`cd /.../.../BTS_Backups/BTS_Backup_mmdd\`

**Note**
In this command, `-p` means to create the directory if it does not exist; but if it does exist, do nothing. In the directory filename, mmdd = month and day.

**Step 6**
Place the applicable backup files in the backup subdirectory.

\`put <backup file name>\`

**Step 7**
After the transfer is complete and the ftp prompt reappears, exit the ftp session.

\`bye\`

Compare Checksums

To compare checksums, perform the following steps:

**Step 1**
Log in to the remote NFS by entering your username and password for that system.

**Step 2**
Navigate to the subdirectory on which the backup files were written.

\`cd /.../.../BTS_Backups/BTS_Backup_mmdd\`
Chapter 26  Backing Up and Restoring the Cisco BTS 10200 Softswitch

Back Up the Cisco BTS 10200 Softswitch

Note
In the directory name, mmdd = month and day.

Step 3  List the files in the backup directory. The following command lists the files in reverse order by creation date.

```
ls -lrt
```

Step 4  Run a checksum on the files that were backed up.

```
cksum <file name>
```

Step 5  Compare these checksum values to the corresponding checksum values that were taken in Step 5 of the Run a Backup of the Cisco BTS 10200 Softswitch, page 26-3.

Step 6  If the checksum values are not the same, repeat Step 2 through Step 5. If the checksum values are still different, contact the Cisco Technical Assistance Center for assistance.  
If the checksum values are the same, you have completed the backup for the current Cisco BTS 10200 Softswitch.

Managing Files In the Backup Directory

Back up files to a remote NFS on a regular basis. In the unlikely event that both sides of a component go down, these backup files are needed to restore the system. Backup files are stored on the local Cisco BTS 10200 Softswitch drives in the /opt/ems/bac kup directory for 7 days. After 7 days, they are automatically erased by the system.

Caution
If you do not back up files via FTP to a remote NFS (as described in this section), files older than 7 days are lost.

If you do too many backups in one day on the system, the available disk space on the local Softswitch Call Agent drive may begin to fill up with daily backup files. If that happens, you can free up disk space by deleting older backup files that you have already transferred (via FTP) to the remote server. Cisco recommends that you monitor the available disk space on a regular basis.

Caution
Do not allow the disk to become filled with old backup files, as this can affect performance.

Backing Up Ulticom OMNI Data

This section describes the procedures for backing up Ulticom OMNI data.

Automatic Backup

Ulticom automatically backs up the SS7 configuration every 5 days. The /opt/omni/conf directory contains files named archive.a7n1.$SHM.DATE, where $SHM is the shared memory value (225) and DATE is yymmdd (for example, archive.a7n1.225.000717). To view these files, log in to the active CA and navigate to the /opt/omni/conf directory.
In addition to the automatic backup, a service provider can back up the Ulticom data at any time by using the following procedure.

**Important Notes About This Procedure**

Throughout this procedure, each command is shown with the appropriate system prompt, followed by the command to be entered in **bold**. The prompt is generally the host system prompt: `<hostname>`#.

The backup procedure uses the following conventions:

- Enter commands as shown, as they are case sensitive.
- Press the **Return** (or **Enter**) key at the end of each command.

**Operator Backup**

This section describes the operator backup procedure.

**Log In to the Active CA as Root User**

To log in to an active Cisco BTS 10200 Softswitch as a root user, perform the following steps.

To communicate with the CA via SSH, perform the following steps in an XTerm window. (If available on your console, you can also use an application tool such as Exceed.)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Ensure that your local PC or workstation has connectivity via TCP/IP to communicate with the standby Cisco BTS 10200 Softswitch unit that you are backing up.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Open a UNIX shell (or, in Windows, choose <strong>Start&gt;Run&gt;Command Prompt</strong>) or XTerm window.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>At the UNIX shell prompt, enter <code>ssh</code>, <code>root</code>, and the host name or domain name of the standby Cisco BTS 10200 Softswitch. <code>ssh -l root &lt;CA host-name&gt;</code> The password prompt appears.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enter the root password. <code>&lt;root password&gt;</code> A <code>&lt;hostname&gt;</code> # prompt appears, where <code>&lt;hostname&gt;</code> is the machine name for the active Cisco BTS 10200 Softswitch.</td>
</tr>
</tbody>
</table>

**Starting the OMNI Stack**

To start the OMNI stack, perform the following steps.

**Note**

The Ulticom Omni stack must be running before you can make a backup. If the Omni stack is not yet running, start it using Step 1. If the Omni stack is already running, go to “Execute Backup Command”.

**Step 1** Start the Omni GUI application.
platform start -i omni

Execute Backup Command

To execute the backup command, perform the following steps:

**Step 1** In the XTerm window for the active CA, navigate to the Omni configuration directory.

```
<hostname># cd /opt/omni/conf
```

**Step 2** Start the termhandler:

```
<hostname># termhandler -node a7n1
```

The system responds with the termhandler prompt:

```
+-------------+    Terminal Handler [Started]
| TermHandler |    Copyright 1993, 1994 DGM&S
+-------------+    All Rights Reserved

Usage: Filename:    - to execute from a file
MML command: - series of mml command(s)
```

**Step 3** Enter the following command followed by a semicolon:

```
OMNI [ddmmyyyy hh:mm:ss] #1:bkup-node;
```

The configuration prompt appears.

**Step 4** Enter `y` to proceed:

```
Send [BKUP-NODE;]? [Y/N]y
```

The system confirms that the backup was completed.

```
Sent MML command #1 to <hostname>.PM, cmd[BKUP-NODE;]
starting 5 min. timer...
1 [ddmmyyyy hh:mm:ss]
BKUP-NODE;
M COMPLETED
Configuration backup completed
```

A backup of the SS7 network configuration is created under filename `archive.a7n1.$SHM.DATE`, where `$SHM` is the shared memory value (225) and `DATE` is `yymmdd` (for example, `archive.a7n1.225.000717`).

**Step 5**Quit Termhandler.

```
OMNI [ddmmyyyy hh:mm:ss] #2:q
```

**Step 6**Display the archive file(s).

```
<hostname># ls -ltr arch*
```

Confirm that the file you just archived is displayed at the end of the list. If there are any questions, contact Cisco TAC.

---

Example 26-1 provides a sample transcript of an Omni backup.
Example 26-1 Transcript of Omni Backup

netra12# termhandler -node a7n1

+-------------+  Terminal Handler [Started]
| TermHandler  |  Copyright 1993, 1994 DGM&S
+-------------+  All Rights Reserved

Usage: Filename:   - to execute from a file
          MML command: - series of mml command(s)


Send [BKUP-NODE;]? [Y/N]y
Sent MML command #1 to netra12.PM, cmd[BKUP-NODE;]
    starting 5 min. timer...
BKUP-NODE;
M COMPLETED
Configuration backup completed

Usage: Filename:   - to execute from a file
          MML command: - series of mml command(s)

netra12# ls -ltr arch*
-rw-r--r--   1 root     other        890 Jul 11 00:00 archive.a7n1.225.000711
-rw-r--r--   1 root     other        890 Jul 16 00:00 archive.a7n1.225.000716
-rw-r--r--   1 root     other        890 Jul 17 13:28 archive.a7n1.225.000717
netra12#

Restoring the Cisco BTS 10200 Softswitch

This section describes how to restore the Cisco BTS 10200 Softswitch.

Caution

This procedure assumes that the Cisco BTS 10200 Softswitch was down. Do not execute this procedure without first contacting Cisco TAC regarding restoring data in the event of disaster recovery.

Refer to the Cisco BTS 10200 Softswitch Element Management System Database Backup and Recovery Procedure feature module for element management system (EMS) data restoral information.

Restore Primary Cisco BTS 10200 Softswitch Shared Memory Data

This section describes how to restore the primary (side A) Cisco BTS 10200 Softswitch shared memory data.

FTP Backup Files to the Primary Cisco BTS 10200 Softswitch

To use FTP to back up files to the primary Cisco BTS 10200 Softswitch, perform the following steps.

Note

Depending upon the security policy of the remote NFS, you may need to use secure FTP (SFTP) to execute these steps.
Restoring the Cisco BTS 10200 Softswitch

Step 1 Log in to the remote NFS by entering your username and password for that system.

Step 2 At the prompt, establish an FTP session with the primary Cisco BTS 10200 Softswitch.

```
ftp xxx.xxx.xxx.xxx
```

The username prompt appears.

Step 3 Enter the user name root.

```
root
```

The password prompt appears.

Step 4 Enter the root password for this machine (host).

```
<password for user root>
```

An ftp prompt appears.

Step 5 Enter bin to enable binary transfer.

```
Note
If you are using SFTP, skip to Step 5.
```

Step 6 On the primary Cisco BTS 10200 Softswitch, navigate to the directory where the restore files will be written.

```
cd /opt/ems/backup
```

Step 7 Place the applicable Cisco BTS 10200 Softswitch restore files in the backup directory.

```
put <restore file name>
exmaple of <restore file name> = CA166.mem.cfg:900-00.01.00.Q07:06192035
```

```
put <restore file name>
exmaple of <restore file name> = CA166:900-00.01.00.Q07:06192035:.tar.gz
```

```
put <restore file name>
exmaple of <restore file name> = FSAIN205.mem.cfg:900-00.01.00.Q07:06192035
```

.....(additional files)

Step 8 After the transfer is complete and the ftp prompt reappears, exit the ftp session.

```
bye
```

Verify That Files Are Transferred

To verify that your backup files are transferred, perform the following steps:

Step 1 Ensure that your local PC or workstation has connectivity via TCP/IP to communicate with the primary Cisco BTS 10200 Softswitch unit that you are backing up.

Step 2 Open a UNIX shell (or, in Windows, choose Start>Run>Command Prompt) or XTerm window.
Step 3  At the UNIX shell prompt, enter `ssh`, `root`, and the host name or domain name of the standby Cisco BTS 10200 Softswitch.

```bash
ssh -l root <host-name>
```

The password prompt appears.

Step 4  Enter the root password.

```
<root password>
```

A `<hostname> #` prompt appears, where `<hostname>` is the machine name for the active Cisco BTS 10200 Softswitch.

### Performing Shared Memory Restore

To restore the shared memory files, perform the following steps:

**Step 1** At the prompt of the primary Cisco BTS 10200 Softswitch machine, navigate to the utils directory.

```
cd /opt/ems/utils
```

**Step 2** Run the backup.

```
./dataBackRes -r
```

*Note*  In this command, `-r` means the restore process.

*Note*  Depending upon the shared data file size, this process can take up to 20 minutes.

**Step 3** Follow and respond to the prompts that the system displays.

### Start Platforms

**Step 1** Use the following command to bring up the primary Cisco BTS 10200 Softswitch.

```
platform start
```

*Caution*  If this procedure is being done after a disk failure, the Omni SS7 network configuration ([Restoring Ulticom Omni Data, page 26-14](#)) must be restarted before you restart the platform.
Step 2 Bring up the secondary Cisco BTS 10200 Softswitch. Ensure that your local PC or workstation has connectivity via TCP/IP to communicate with the secondary Cisco BTS 10200 Softswitch unit that you are backing up.

Step 3 Open a UNIX shell (or, in Windows, choose Start>Run>Command Prompt) or XTerm window.

Step 4 At the UNIX shell prompt, enter `ssh`, `root`, and the host name or domain name of the standby Cisco BTS 10200 Softswitch.

Note: It is best to use the secondary (not the active) Cisco BTS 10200 Softswitch machine, because the file transfer in this procedure can take up to 10 minutes.

```
ssh -l root <host-name>
```

The password prompt appears.

Step 5 Enter the root password.

```
<root password>
```

A `<hostname>` # prompt appears, where `<hostname>` is the machine name for the secondary Cisco BTS 10200 Softswitch.

Step 6 Use the following command to bring up the secondary Cisco BTS 10200 Softswitch.

```
platform start
```

Caution: If this procedure is being done after a disk failure, the Omni SS7 network configuration (Restoring Ulticom Omni Data, page 26-14) must be restarted before you restart the platform.

Check System Status

This section describes how to check the primary Cisco BTS 10200 Softswitch system status to ensure that your files have been restored.

Log In to the Primary EMS for CLI Session

Step 1 Ensure that your local PC or workstation has connectivity via TCP/IP to communicate with the primary Cisco BTS 10200 Softswitch.

Step 2 Open a UNIX shell (or, in Windows, choose Start>Run>Command Prompt) or XTerm window.

Step 3 At the UNIX shell prompt, enter `ssh`, `optiuser`, and the hostname of the primary EMS.

```
ssh -l optiuser <primary EMS hostname>
```

A password prompt appears.

Step 4 Enter the password for optiuser.

```
<password for optiuser>
```

A CLI prompt appears.
Check for Alarms on the System

To check for any system alarms, perform the following steps:

**Step 1**
Show any alarms.

```
show alarm
```

The system responds with all current alarms, which must be verified or cleared before executing this upgrade procedure.

**Tip**
Use the following command information for reference ONLY.

**Step 2**
Use the following command example to continuously monitor system alarms.

```
subscribe alarm-report severity=all; type=all;
```

**Note**
Valid severities are: MINOR, MAJOR, CRITICAL, ALL. Valid types are: CALLP, CONFIG, DATABASE, MAINTENANCE, OSS, SECURITY, SIGNALING, STATISTICS, BILLING, ALL, SYSTEM, AUDIT.

The system displays any reported alarms.

Example response:

```
CLIS------------------------------- START ALARM REPORT -------------------------
TIMESTAMP: Fri Mar 14 14:01:28 CST 2003
DESCRIPTION: Disk Partition Moderately Consumed
TYPE & NUMBER: MAINTENANCE (90)
SEVERITY: MINOR
ALARM-STATUS: ON
ORIGIN: <hostname>
COMPONENT-ID: HMM
Disk Partition: /
Percentage Used: 54.88
-------------------- END ALARM REPORT ------------------------
```

**Step 3**
Use the following command example to stop monitoring system alarms.

```
unsubscribe alarm-report severity=all; type=all;
```

**Step 4**
Exit the CLI.

```
exit
```

You have completed restoration of system data. Proceed to the “Restoring Ulticom Omni Data” section on page 26-14 if you need to restore Ulticom data.
Restoring Ulticom Omni Data

This section describes how to restore the Ulticom Omni data. This procedure restores Omni data from a saved backup file. This is only necessary if both the active CA and standby CA Omni data have been corrupted.

As described in the procedure, the currently loaded Omni configuration must first be deleted (zeroed out). Then the configuration must be restored from the backup file.

Important Notes About This Procedure

Throughout this procedure, each command is shown with the appropriate system prompt (for example, <hostname>#), followed by the command to be entered in bold.

Use the following conventions throughout the steps in this procedure:

- Enter commands as shown, as they are case sensitive.
- Press the Return (or Enter) key at the end of each command.

Restore Procedure

This section describes how to restore the Omni configuration.

Log In to the Active CA as Root User

To communicate with the Cisco BTS 10200 Softswitch using SSH, perform the following steps in an XTerm window. (If available on your console, you can also use an application tool such as Exceed.)

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Ensure that your local PC or workstation has connectivity via TCP/IP to communicate with the standby Cisco BTS 10200 Softswitch unit that you are backing up.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Open a UNIX shell (or, in Windows, choose Start&gt;Run&gt;Command Prompt) or XTerm window.</td>
</tr>
<tr>
<td>Step 3</td>
<td>At the UNIX shell prompt, enter ssh, root, and the host name or domain name of the standby Cisco BTS 10200 Softswitch.</td>
</tr>
<tr>
<td></td>
<td>ssh -l root &lt;CA host-name&gt;</td>
</tr>
<tr>
<td></td>
<td>The password prompt appears.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the root password.</td>
</tr>
<tr>
<td></td>
<td>&lt;root password&gt;</td>
</tr>
<tr>
<td></td>
<td>A &lt;hostname&gt; # prompt appears, where &lt;hostname&gt; is the machine name for the active Cisco BTS 10200 Softswitch.</td>
</tr>
</tbody>
</table>

Stop the Application and Delete the Existing Configuration

To stop the Cisco BTS 10200 Softswitch CA application and delete the existing configuration, perform the following steps:
Step 1  Stop the Cisco BTS 10200 Softswitch CA application (this is required, because the designated process, a7n1_ctrl is deleted in the steps that follow).

<hostname>#$ platform stop -i

Note  You must execute a platform stop on both the primary and secondary systems.

System response:
Terminating platform pmg.CAxxx............
Platform pmg.CAxxx is terminated successfully...

Step 2  Navigate to the Omni configuration directory.

   cd /opt/omni/conf

Step 3  Run the configureNodes script to delete the configuration:

<hostname>#$ configureNodes -clean

Note  Perform Step 3 on both the primary and secondary systems.

Step 4  Run the configureNodes script to initialize the configuration:

<hostname>#$ configureNodes a7n1 A7

Note  Perform Step 4 on both the primary and secondary systems.

Start the Omni Stack and Restore Omni Data from the Backup File

In the XTerm window for the active Cisco BTS 10200 Softswitch CA, enter the following commands at the hostname prompt:

Step 1  Start the Omni stack.

<hostname>#$ platform start -i omni

Step 2  Start Termhandler:

<hostname>#$ termhandler -node a7n1

The system responds with the termhandler prompt:

+-----------------+    Terminal Handler [Started]
| TermHandler     |    Copyright 1993, 1994 DGM& S
+-----------------+    All Rights Reserved

Usage: Filename:   - to execute from a file
        MML command: - series of mml command(s)

Step 3  Enter the full path name to the backup file, followed by a semicolon.

OMNI [ddmmyyyy hh:mm:ss] #1:/opt/omni/conf/archive.a7n1.225.yymmdd;
Step 4  At the display response from each command prompt, enter y. The configuration will be restored from the backup file.

Step 5  Enter the following command to quit the Omni application and return to the host prompt:

    OMNI [ddmmyyyy hh:mm:ss] #2:q

Start the Cisco BTS 10200 Softswitch Application

To start the Cisco BTS 10200 Softswitch application, perform the following steps:

Step 1  Start the Cisco BTS 10200 Softswitch application.

    <hostname># platform start

System response:

    Starting platform pmg.CAxxx...
    It may take up to 5 minutes.......  
    Platform pmg.CAxxx Started and its in STANDBY state...

    <hostname>#