Software Input Output Reference — Maintenance
Avaya Communication Server 1000

7.5
NN43001-711, 05.04
April 2011

© 2011 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Preventing Toll Fraud

“Toll fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud Intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: New in this release....11
- Other changes....13
  - Revision History....13

Chapter 2: Customer service....17
- Navigation....17
- Getting technical documentation....17
- Getting product training....17
- Getting help from a distributor or reseller....17
- Getting technical support from the Avaya Web site....18

Chapter 3: Introduction....19
- Note on legacy products and releases....19
- Subject....19
- Format and structure....19
  - The Basic commands Table....20
  - The Alphabetical list of commands Table....20
- Applicable systems....21
  - System migration....21
- Intended audience....22
- Conventions....22
  - Terminology....22
  - Notational conventions....23
- Related information....24
  - Documentation....24
  - Online....24

Chapter 4: Communicating with the system....25
- Changing the IP scheme on the ELAN....25
- Accessing the system....26
  - Logging in and out....26
  - Local and remote access....26
  - HOST mode access....27
  - Line mode interface log in procedure....27
  - Access through the maintenance telephone....28
  - Accessing Meridian Mail....30
- System memory and disk space....30
  - Legend:....30
  - Low memory and disk warnings....31
- System Look up messages....31
- Multi-User Login....32
  - User commands....32
- Maintenance display codes....33
- Time and date of fault....33
- Applications that use SFTP....33

Chapter 5: Alphabetical list of packages....35

Chapter 6: Overlay loader and Multi-User Login....47

Overlay loader....47
Overlay loader commands....47
Multi-User Login commands....48
Multi-User commands....48

Chapter 7: LD 01: Template audit....51
Consistency Checks....51
User Count Scan....51
Duplicate Template Scan....51
Template Checksum Audit....52
Key Lamp Strip Audit....52
Template Pointer Audit....52
Operating parameters....52
Sample operation....53

Chapter 8: LD 30: Network and Signaling Diagnostic....55
Program operation....55
How to use LD 30....56
Fibre Network Fabric....56
Basic commands....57
Contents....57
Large System and Avaya Communication Server 1000E commands....57
Superloop commands....58
Basic Rate Interface (BRI) commands....58
Alphabetical list of commands....59

Chapter 9: LD 31: Telephone and Attendant Console Diagnostic....65
M2006 and M2008 Telephone test....65
M2216, M2016S, and M2616 Telephone test....68
M2317 Telephone test....71
M2250 Console test....75
M2250 Console test....77

Chapter 10: LD 32: Network and Peripheral Equipment Diagnostic....81
Overlay 32 linkage....82
Using Enable/Disable commands....83
Fibre Network Fabric....83
Basic commands....84
Contents....84
Basic commands....84
Large System and Avaya Communicatuon Server 1000E System commands....85
Superloop commands....87
ISDN BRI MISP commands....88
ISDN BRI SILC/UILC commands....89
ISDN BRI BRSC commands....90
System commands....91
Alphabetical list of commands....92
Output Example:....122

Chapter 11: LD 33: Peripheral Equipment Diagnostic for Fiber Remote IPE....135
Fiber Remote IPE diagnostic....135
Midnight routine operation....135

Fibre Network Fabric....136
Basic commands for Fiber Remote IPE....136
Alphabetical list of commands....137

Chapter 12: LD 34: Tone and Digit Switch and Digitone Receiver Diagnostic....143
Fibre Network Fabric....143
Basic commands....144
Contents....144
Large System and Avaya Communication Server 1000E System commands....144
Extended Tone Detector (XTD) commands....145
Maintenance telephone commands....146
Alphabetical list of commands....147

Chapter 13: LD 36: Trunk Diagnostic....155
When to use LD 36....155
Trunk error thresholds....156
Fibre Network Fabric....156
Basic commands (LD 36)....157
Alphabetical list of commands....158

Chapter 14: Input/Output Diagnostic....161
Intelligent links (APL, HSL, and LSL)....161
D-channel Expansion....162
Basic commands....162
Multipurpose Serial Data Link (MSDL) commands....164
Alphabetical list of commands....164

Chapter 15: LD 38: Conference Circuit Diagnostic....167
Fibre Network Fabric....167
Basic commands....168
Alphabetical list of commands....168

Chapter 16: LD 39: Intergroup Switch and System Clock Generator Diagnostic....173
Group, loop, and Peripheral Signaling card relationship....173
Fibre Network Fabric....174
Basic commands....174
Alphabetical list of commands....176

Chapter 17: LD 43: Equipment Datadump....183
When the datadump fails....183
Low memory warning....183
Basic commands....184
Alphabetical list of commands....185

Chapter 18: LD 44: Software Audit....189
Running software audit....189

Chapter 19: LD 45: Background Signaling and Switching Diagnostic....191
Using the manual extended continuity (XCON) command....191
Fibre Network Fabric....192
Basic commands....195
XCON sub-prompts....196
Alphabetical list of commands....200

Alphabetical list of XCON sub-prompts....202

Chapter 20: LD 46: Multifrequency Sender Diagnostic for Automatic Number Identification....205

Fibre Network Fabric....205
Basic commands....206
Alphabetical list of commands....206

Chapter 21: LD 48: Link Diagnostic....209

Automatic Call Distribution Links....209
ACD High speed and low speed link monitor....209
APL monitor....209
Integrated Messaging System Links....210
Command and Status Links (CSL)....210
Multi-purpose Serial Data Link (MSDL)....210
Application Module Link (AML)....211
AML/CSL monitor....211
ISDN BRI monitor....211
Single Terminal Access (STA)....211
Voice Mailbox Administration (VMBA)....211
Fibre Network Fabric....212
D-channel Expansion....212
Basic commands....212
Contents....212
Basic commands....213
ACD High speed and low speed link commands....217
ACD High speed and low speed link monitor commands....218
AML commands....218
AML over Ethernet (ELAN subnet) commands....219
AML/CSL monitor commands....220
Auxiliary Processor Link (APL) commands....221
APL monitor commands....222
D-channel Expansion commands....222
Intercept Computer Update (ICU) commands....224
ISDN BRI monitor commands....225
Multipurpose Serial Data Link (MSDL) commands....226
Single Terminal Access (STA) commands....226
Voice Mailbox Administration (VMBA) commands....227
Alphabetical list of commands....227

Chapter 22: LD 51: Intercept Computer Update....259

Basic commands....259
Alphabetical list of commands....259

Chapter 23: LD 54: Multifrequency Signaling Diagnostic....261

Hardware Initialization after SYSLOAD....261
Loop around test during daily routines....262
Loop around test by command....262
MFC/MFE error handler and counter....263
Fibre Network Fabric....263
Basic commands....263
Alphabetical list of commands....264

Chapter 24: LD 60: Digital Trunk Interface and Primary Rate Interface Diagnostic.....267
Channel Timeslot Mapping.....267
Fibre Network Fabric.....268
Basic commands.....268
DTI/PRI commands.....268
Clock controller commands.....269
Alphabetical list of commands.....270

Chapter 25: LD 61: Message Waiting Lamps Reset.....281
G command.....281

Chapter 26: LD 75: Digital Trunk Maintenance.....283
Basic commands.....283
Alphabetical list of commands.....285

Chapter 27: LD 77: Manual Print.....289
When to use LD 77.....289
LD 77 Output format.....289
Abbreviations for LD 77.....290
LD 77 Input format.....290
Fibre Network Fabric.....291
Basic commands.....291
Alphabetical list of commands.....292

Chapter 28: LD 80: Call Trace.....299
Enhanced Trace commands.....299
Calling Line ID on Analog Trunks for Singapone, Australia and Hong Kong.....300
When to use LD 80.....300
Originating and terminating information.....301
Example 1 Trace a call placed to a 500-type set.....301
Example 2 Trace an outgoing ISDN call.....302
Example 3 Enhanced Trace command output.....302
Example 4 Trace a call from an IP Media Services Ad Hoc Conference loop:.....303
VoIP Trace command output.....303
Example 1 Trace a call placed from IP Phone to IP Phone within a single system.....304
Example 2 Trace a Outgoing Virtual Trunk Call between TDM Phone and VGW Resource on Different Systems.....304
Example 3 Trace an Incoming Virtual Trunk Call between two different systems.....305
Example 4 Trace an IP Phone to Local TDM Device.....305
Example 5 Trace a call scenario between two Avaya Communication Server 1000E Media Gateways: 306
Alphabetical list of Call Trace outputs.....306
Basic commands.....310
Small Systems, CS 1000S, MG 1000B, and MG 1000T commands.....311
Alphabetical list of commands.....312

Chapter 29: LD 92: Automatic Trunk Maintenance.....317
Basic commands.....317
Alphabetical list of commands.....318

Chapter 30: LD 96: D-channel Diagnostic.....321
Monitoring.....321
D-channels.....321

B-channels and ISL channels....322
ISDN features....322
D-channel DN tracing....323
Message types....324
Setting output format levels....325
Deactivate monitor from a maintenance telephone....327
Get monitor status....328
Example: Status of D-channel monitor....328
Multi-purpose Serial Data Link (MSDL)....328
D-channel Expansion....329
CS 1000S Survivable IP....329
D-channel commands....329
D-channel Expansion commands....332
Multipurpose Serial Data Link (MSDL) commands....335
Multipurpose Serial Data Link D-channel commands....336
D-channel call trace commands....336
Outgoing messages....337
Incoming messages....338
Alphabetical list of commands....339

Chapter 31: LD 117: Ethernet and Alarm Management....361
Command format....361
Alarm Management capability....362
Feature packaging....362
The Event Collector....362
The Event Server....362
Escalation and suppression thresholds....364
Global window timer length....364
TTY output format of events....364
Fancy format output....364
Unformatted Output....365
Ethernet and Point-to-Point Protocol....366
How to Configure Ethernet and Point-to-Point Protocol....366
Command descriptions....369
Object descriptions....369
How to configure IP Connectivity with CS 1000S....370
Point-to-Point configuration - Call Server, Bootp is used....371
Recommended BootP configuration for Layer 2 LAN configuration - Call Server only....371
Manual Layer 2 configuration - Call Server and MG 1000S....372
Manual Layer 3 configuration - Call Server and MG 1000S....374
Auto-Negotiate on 100BaseT ports....376
IP command descriptions....377
NTP Command descriptions....392
Alphabetical list of Administration commands....393
Alphabetical list of Maintenance commands....485

Chapter 32: LD 135: Core Common Equipment Diagnostic....501
Possible OOS messages....501
Adding a group to an Option 81C/81C CPII....502
Basic commands....502
Alphabetical list of commands....505

Chapter 33: LD 137: Core Input/Output Diagnostic.....515
Basic commands.....516
Alphabetical list of commands.....518

Chapter 34: LD 143: Customer Configuration Backup and Restore.....527
Basic commands.....527
Alphabetical list of commands.....529

Chapter 35: Media Card command line interface commands.....539
Contents.....539
Introduction.....540
Overview.....540
ITG-SA command line interface commands.....541
OAM security shell commands.....541
PDT security shell commands.....561
MC32S Command Line Interface commands.....561
OAM security shell commands.....561
PDT security shell commands.....569

Chapter 36: Media Gateway Controller command line interface commands.....581
Contents.....581
Introduction.....582
Level One (OAM) CLI commands.....582
OAM Command groups.....582
OAM Commands.....583
Level Two (LDB) CLI commands.....591
LDB Command groups.....591
LDB Commands.....592

Chapter 37: Signaling Server Command Line Interface commands.....599
Contents.....599
Introduction.....600
Level One (OAM) CLI commands.....601
OAM Command groups.....601
OAM Commands.....604
Level Two (PDT) CLI commands.....645
PDT Command groups.....645
PDT Commands.....647
Accounts commands: user account administration commands.....647
PDT built-in commands: PDT built-in.....647
PDT Patcher commands: patcher.....648
PDT RID commands: remote iset diagnostics.....650
PDT cds commands: Converged Desktop Service module.....650
disk commands: file system maintenance and diagnostics.....652
PDT nrsDB commands: Network Routing Service.....652
rdtools commands: rd tools.....655
PDT sipnpm commands: SIP Network Protocol Module.....656
PDT system commands: System administration.....658
PDT ums commands : UMS module commands.....660
PDT iset commands: iset module commands.....661
CLI commands in Linux.....663

Chapter 38: UDT Universal Digital Trunk card Command Line Interface.....665
Command Line Interface.....665
Main menu.....666
ls command.....667
? command.....667
System Maintenance.....667
ls command.....668
? command.....668
System Test.....668
crestart command.....669
mreport command.....670
showerr command.....670
qver command.....671
ttad command.....672
stad command.....672
UDT Administration.....672
ls command.....673
? command.....673
E1T1Settings command.....673
UDT Maintenance.....674
ls command.....674
? command.....675
Alarm Status command.....675
ChannelStatus command.....675
Lpbck command.....676
PLLStatus command.....676
SpanStatus command.....676
UdtConfig command.....677
Remote access to the UDT card.....677

Chapter 39: Linux base CLI commands.....679

Index.....687

Chapter 1: New in this release

The following sections detail what's new in this document for Avaya Communication Server 1000 Release 7.5.

LD 80: Call Trace for Extended Local Calls

VoIP Trace command output

```
Trace command:
.trac 0 79005

Output:

ACTIVE  VTN 120 0 00 05

EXTENDED LOCAL CALL:

ORIG   VTN 120 0 00 05  KEY 0  SCR MARP  CUST 0  DN 79005  TYPE 1230
  SIGNALLING ENCRYPTION: INSEC
  MEDIA ENDPOINT IP: 192.168.30.147  PORT: 5200
TERM   VTN+E1 104 0 13 31   VTRK IPTI  RMBR  19 32 OUTGOING VOIP GW CALL
  FAR-END SIP SIGNALLING IP: 192.168.36.85
  FAR-END MEDIA ENDPOINT IP: 192.168.61.28  PORT: 50002
  FAR-END VendorID:Avaya CS1000 SIP GW release_7.0 version_ssLinux-7.50.07
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT  N/A  TXPT  N/A  DIAL DN 79777
MAIN_PM  ESTD
TALKSLOT  ORIG  12   TERM  49
QUEU  NONE
CALL ID 616 19044
---- ISDN ISL CALL (TERM) ----
CALL REF # =  2415
BEARER CAP =  VOICE
HLC =
CALL STATE =  10    ACTIVE
CALLING NO =  79005  NUM_PLAN:PRIVATE    TON:ABBREVIATED  ESN:CDP
CALLED NO  =  79777  NUM_PLAN:PRIVATE    TON:ABBREVIATED  ESN:CDP

ORIG   VTN 104 0 13 00   VTRK IPTI  RMBR  19 1 INCOMING VOIP GW CALL
  FAR-END SIP SIGNALLING IP: 192.168.36.85
  FAR-END MEDIA ENDPOINT IP: 192.168.30.147  PORT: 5200
  FAR-END VendorID: Avaya  CS1000 SIP GW release_7.0 version_ssLinux-7.50.07
TERM   VTN 120 0 00 22  KEY 0  SCR MARP  CUST 0  DN 79777  TYPE SLUEXT
  SIGNALLING ENCRYPTION: INSEC
  UEXT PROXY VTN 104 0 14 09   VTRK IPTI  RMBR  3 10 OUTGOING VOIP GW CALL
  FAR-END SIP SIGNALLING IP: 0.0.0.0
  FAR-END MEDIA ENDPOINT IP: 0.0.0.0  PORT: 0
  FAR-END VendorID: Avaya IP Softphone 3456 release 2.6 stamp 57666
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT  N/A  TXPT  N/A  DIAL DN 79777
MAIN_PM  ESTD
TALKSLOT  ORIG  24   TERM  29
QUEU  NONE
CALL ID 616 19043
NETWORK  CALL ID  616 19044
---- ISDN ISL CALL (ORIG) ----
CALL REF # =  2614
BEARER CAP =  VOICE
HLC =
CALL STATE =  10    ACTIVE
CALLING NO =  79005  NUM_PLAN:PRIVATE    TON:ABBREVIATED  ESN:CDP
CALLED NO  =  79777  NUM_PLAN:PRIVATE    TON:ABBREVIATED  ESN:CDP
```

Alphabetical list of Call Trace outputs

EXTENDED LOCAL CALL is printed out if call traces are printed for Extended Local Call.

Other changes

There are no other changes in this release.

Revision History

April 2011	Standard 05.04. This document is up-issued to support Avaya Communication Server 1000 Release 7.5. Added SCHD to GRDRC in LD 117.
January 2011	Standard 05.03. This document is up-issued to support Avaya Communication Server 1000 Release 7.5. Various commands associated with obsolete features are removed.
December 2010	Standard 05.02. This document is up-issued to support Avaya Communication Server 1000 Release 7.5. Various commands associated with obsolete features are removed.
November 2010	Standard 05.01. This document is up-issued to support Communication Server 1000 Release 7.5.
July 2010	Standard 04.02. This document is up-issued to support Communication Server 1000 Release 7.0.
June 2010	Standard 04.01. This document is up-issued to support Communication Server 1000 Release 7.0.
March 2010	Standard 03.12. This document is up-issued to reflect changes made to the section LD 117: Ethernet and Alarm Management.
February 2010	Standard 03.11. This document is up-issued to reflect changes made to the section AML/CSL monitor commands.
February 2010	Standard 03.10. This document is up-issued to reflect changes made to the section Overlay 48 commands.
January 2010	Standard 03.09. This document is up-issued to reflect changes made to the section LD 117: Time Interval.
December 2009	Standard 03.08. This document is up-issued to reflect changes made to the section LD117: Ethernet and Alarm Management.
October 2009	Standard 03.07. This document is up-issued to support MG XPEC.
September 2009	Standard 03.06. This document is up-issued to update the section D-channel call trace commands.

July 2009 Standard 03.05. This document is up-issued to support Communication Server 1000 Release 6.0.

June 2009 Standard 03.04. This document is up-issued to support Communication Server 1000 Release 6.0.

June 2009 Standard 03.03. This document is up-issued to support Communication Server 1000 Release 6.0.

May 2009 Standard 03.02. This document is up-issued to support Communication Server 1000 Release 6.0.

May 2009 Standard 03.01. This document is up-issued to support Communication Server 1000 Release 6.0.

January 2009 Standard 02.11. This document is up-issued to reflect changes in technical content in section Communicating with the system.

November 2008 Standard 02.10. This document is up-issued to reflect changes in technical content in section Alphabetical list of Administration commands.

October 2008 Standard 02.09. This document is up-issued to reflect changes in technical content.

October 2008 Standard 02.08. This document is up-issued to reflect changes in technical content.

October 2008 Standard 02.07. This document is up-issued to reflect changes in technical content.

September 2008 Standard 02.06. This document is up-issued to reflect changes in technical content in the section LD 60: Digital Trunk Interface and Primary Rate Interface Diagnostic.

April 2008 Standard 02.05. This document is up-issued for editing changes.

March 2008 Standard 02.04. This document is up-issued for editing changes.

March 2008 Standard 02.03. This document is up-issued to support Communication Server 1000 Release 5.5.

January 2008 Standard 02.02. Up-issued to reflect changes in technical content.

In LD117:

- in STIP TYPE command, removed "1240" as an argument
- added CHG SUPPRESS_ALARM command with arguments and description
- in CHG ADMIN_COMM command, changed indicated value for DEFAULT(1) from "Public" to “admingroup1”
- in PRT SEL command

  removed "ALL" as an argument (Category) and indicated that ALL is the default when no Category argument is specified

- added PRT SUPPRESS_ALARM command with arguments and description
- added TEST ALARM command with arguments and description

December 2007 Standard 02.01. Up-issued to support Communication Server 1000 Release 5.5.

November 2007 Standard 01.07. Up-issued to reflect changes in technical content. In LD117, syntax of an argument for the SYNC NTP command changed from BKGD to BACKGROUND.

October 2007 Standard 01.06. Up-issued to reflect changes in technical content.

July 2007 Standard 01.05. Up-issued to reflect changes in technical content.

June 2007 Standard 01.04. Up-issued to reflect changes in technical content.

June 2007 Standard 01.03. Up-issued to reflect changes in technical content.

May 2007 Standard 01.02. Up-issued to reflect changes in technical content.

March 2007 Standard 01.01. Up-issued to support Communication Server 1000 Release 5.0.
This document contains information previously contained in the following legacy document, now retired: Software Input/Output: Maintenance (553-3001-511).

October 2006 Standard 15.00. This document is up-issued to reflect changes in technical content.

- LD32 - STAT command expanded.
- LD43 - clarification of Datadump / Datadownload process.
- LD80 - TRCR command added.

July 2006 Standard 14.00. Up-issued to reflect changes in technical content.

- LD117 - ZDST: Note concerning last week of the month value = 5.
- LD117 - SHELLS: Warning concerning disabling shells.
- LD143 - KSTT, KSHO, KDIF, KNEW, KRVR, KOUT, KUPL: New definitions added and procedure for CP PIV.

August 2005 Standard 13.00. Up-issued to support Communication Server 1000 Release 4.5.

September 2004 Standard 12.00. Up-issued to support Communication Server 1000 Release 4.0.

October 2003 Standard 11.00. Up-issued to support Succession 3.0.

November 2002 Standard 10.00. Up-issued to include content changes for Meridian 1 Release 25.4x and Succession Communication Server for Enterprise 1000, Release 2.0.

January 2002 Standard 9.00. This is a global document and is up-issued for Release 25.40.

December 2000	Standard 8.00. Up-issued for X11 Release 25.3x and now contains information on small system IP Expansion.
April 2000	Standard 7.00. This is a global document and is up-issued for X11 Release 25.0x. Document changes include removal of: redundant content; references to equipment types except Options 11C, 51C, 61C and 81C; and references to previous software releases.
June 1999	Standard 6.00. Up-issued to include updates and changes required for X11 Release 24.2x.
March 1999	Standard 5.00. Up-issued to include updates and changes required for X11 Release 24.0x.
October 1997	Standard 4.00. Up-issued to include updates and changes required for X11 Release 23.0x.
August 1996	Standard 3.00. Up-issued to include updates and changes required for X11 Release 22.0x.
December 1995	Standard 2.00. Up-issued to include updates and changes required for X11 Release 21.1x.
July 1995	Standard 1.00. This document is issued to include updates and changes required for X11 Release 21.0x. This document has a new number 553-3001-511 and replaces document number 553-2301-511.

Chapter 2: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

- Getting technical documentation on page 17
- Getting product training on page 17
- Getting help from a distributor or reseller on page 17
- Getting technical support from the Avaya Web site on page 18

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, go to www.avaya.com/support. From this Web site, locate the Training link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Chapter 3: Introduction

This document is a global document. Contact your system supplier or your Avaya representative to verify that the hardware and software described are supported in your area.

Note on legacy products and releases

This document contains information about systems, components, and features that are compatible with Avaya Communication Server 1000 software. For more information on legacy products and releases, click the

Technical Documentation link under **Support** on the Avaya home page:

www.avaya.com

Subject

This document covers system commands that are entered to:

- view and print status of switch information
- perform background tests
- disable, enable and test system hardware (e.g. a particular phone)

When a data administrator loads a Maintenance overlay into memory on a Terminal, the administrator may then type in any command documented in that overlay. The system responds to command entries either by changing the status of hardware or by presenting information on the Terminal. (The term "overlay" is synonymous with the terms "load" and "overlay program".)

A list of available Feature Packages is included in this document. An alphabetical listing (sorted by Package mnemonic) of Feature Packages can be found in Alphabetical list of packages on page 35.

Format and structure

This document presents only maintenance overlays and text supplementary to these overlays. Overlay programs are identified by LD XX or LD XXX where XX or XXX is the overlay number.

Maintenance overlays are arranged in numerical order and appear in this document as separate modules.

Two general tables appear in each Load. The first general table is titled "Basic commands". It appears at the front of each load and often follows introductory text. The second general table concludes each Maintenance Load and is titled "Alphabetical list of commands".

The Basic commands Table

This table presents an abbreviated listing of that load's entire command selection. A brief description of the command is presented beside each command.

Shown below is an excerpt from a "Basic commands" table:

CDSP	Clears the maintenance display on active CPU to ....
CMIN	Clears minor alarm for all customers
CMIN ALL	Clears minor alarm for all customers

Note that in a Basic commands table:

- There are no column headings.
- The list is always arranged in alphabetical order.
- The corresponding comment is typically brief.

"Basic commands" are presented in more detail in the "Alphabetical list of commands" table.

The Alphabetical list of commands Table

This table provides a more detailed description of a given command. Shown below is an excerpt from an Alphabetical list of commands table:

Command	Description	Pack/Rel
DISI loop c	Disable carrier c on RPE loop when idle. The number of channels still busy on the carrier may be checked using the STAT command. The message ...	rpe-1
LOCK x	Lock IP Expansion cabinet or Media Gateway in its operating mode. Where x is: 1, 2, 3, or 4	
	For Small System For CS 1000S For MG 1000T	sipe-25 basic-1.0 basic-4.00

Note that in an Alphabetical list of commands table:

- The description is often expansive.
- The package and release column provides the mnemonic of the package that must be equipped on the switch in order to receive this prompt. (In this example, the "rpe" package must be equipped to enter the DISI loop c command.) The number following the hyphen ("1" in this example) denotes the Release of software in which the package was made available.
- The package and release column provides the mnemonic of the package that must be equipped on the switch in order to receive this prompt. (In this example, the "basic" package must be equipped to view REQ.) The number following the hyphen ("1" in this example) denotes the Release of software in which the package was made available. When there are two or more entries in the package and release column for a prompt, the Description column provides clarification. In this example, the command LOCK x was introduced to Small Systems with "sipe-25", to CS 1000S with "basic-1.0" and MG 1000T with basic-4.00.

Applicable systems

This document applies to the following systems:

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)
- Meridian 1 PBX 61C
- Meridian 1 PBX 81C

Note:
When upgrading software, memory upgrades can be required on the Signaling Server, the Call Server, or both.

System migration

When particular Meridian 1 systems are upgraded to run Avaya CS 1000 software and configured to include a Signaling Server, they become CS 1000 systems. Table 1: Meridian 1 systems to CS 1000 systems on page 22 lists each Meridian 1 system that supports an upgrade path to a CS 1000 system.

Table 1: Meridian 1 systems to CS 1000 systems

This Meridian 1 system...	Maps to this CS 1000M system
Meridian 1 PBX 11C Chassis	CS 1000E
Meridian 1 PBX 11C Cabinet	CS 1000E
Meridian 1 PBX 61C	CS 1000M Single Group
Meridian 1 PBX 81C	CS 1000M Multi Group

For more information, see the following documentss:

- *Avaya CS 1000M and Meridian 1 Large System Upgrades Overview, NN43021-458*
- *Avaya Communication Server 1000E Upgrades, NN43041-458*
- *Avaya Communication Server 1000E Upgrade - Hardware Upgrade Procedures, NN43041-464*

Intended audience

This document is intended for individuals responsible for the maintenance of CS 1000 and Meridian 1 systems.

Conventions

Terminology

In this document, the following systems are referred to generically as "system":

- Communication Server 1000E (CS 1000E)
- Communication Server 1000M (CS 1000M)
- Meridian 1

The following systems are referred to generically as "Large System":

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Meridian 1 PBX 61C
- Meridian 1 PBX 81C

In this document, the following circuit cards are referred to generically as Gateway Controller:

- Media Gateway Controller (MGC) card
- Common Processor Media Gateway (CP MG) card
- Media Gateway Extended Peripheral Equipment Controller (MG XPEC) card

In this document, the commands for MGC apply to all Gateway Controller platforms unless otherwise specified.

Notational conventions

Both upper and lower case are used in this book to distinguish between Prompts, Commands, and Variables. Lowercase variables are used in this book to represent many possible responses. The following table lists a few key variables that appear throughout this document:

Variable	Meaning
aa	Text string
aaa bbb	Alphabetic or alphanumeric characters
c	Customer Number
c (u)	Small System, CS 1000S, MG 1000B, and MG 1000T Terminal Number (TN) Card, Unit; where unit is optional
c u	Small System, CS 1000S, MG 1000B, and MG 1000T Terminal Number (TN) Card and Unit
c 0 0 u	Terminal Number (TN) for Small System, CS 1000S, MG 1000B, and MG 1000T. A TN consists of a card, two filler digits, and a unit.
dn	Directory Number (DN)
hh mm	Hours (0 - 23) and Minutes (00 - 59)
loop	Network Loop Number
l s c (u)	Large System and CS 1000E Terminal Number (TN), Loop, Shelf, Card, Unit; where unit is optional
l s c u	Large System and CS 1000E Terminal Number (TN) (loop, shelf, card, and unit number)
mmm	Month (JAN - DEC) when used in a date.
nnn xxx	Numeric characters
xxx	Numeric value of set number of digits
x...x	Numeric value of several digits
yy mm dd	Year (00 - 99), Month (1 - 12) and Day (1 - 31)

<CR> denotes that the carriage return key is to be depressed without inputting any data. The carriage return leaves the existing value unchanged, or enters the default value if there is no existing value.

<space> denotes that the space bar is to be depressed instead of <CR>.

<value> denotes a variable value, generally for a prompt response.

For example, *<NIPN>* is the value responded to the NIPN prompt and *<min>* is a minimum value.

Default values are shown in parentheses.

A range of numbers is denoted by giving the lower and upper limits of the range. For example, given the range 0 - (2) - 3, the user may manually enter 0, 1, 2, or 3, or carriage return (press <CR>) to enter the default of 2.

Default values are shown in brackets in the response column where applicable. Pressing <CR> enters the default.

Where applicable, precede an entry with an X to delete that entry or set your entry to default value.

Related information

This section lists information sources that relate to this document.

Documentation

The following technical publications are referenced in this document:

- *Avaya Features and Services, NN43001-106* contains information on features and the testing of features and services for telephone sets and attendant (ATT) consoles.
- *Avaya Software Input/Output Reference - Administration, NN43001-611* contains information on Administration overlay programs.
- *Avaya Software Input/Output Reference - System Messages, NN43001-712* contains information on system error messages.

Online

To access Avaya documentation online, click the **Documentation** link under **Support** on the Avaya home page: www.avaya.com

Chapter 4: Communicating with the system

To communicate with the system, the following input/output devices at either on-site (local) or remote locations are required:

- TTY or VDT terminal as an input/output device
- RS-232-C compatible printer as an output only device
- Maintenance telephone set as an input only device
- Element Manager for Avaya CS 1000E, Avaya Communication Server 1000S and AvayaCS 1000M
- Optivity Telephony Manager (OTM)

The input/output system can operate with terminals having the following characteristics:

- Interface: RS-232-C
- Code: ASCII
- Speed: 110, 300, 1200, 2400, 4800, and 9600 baud
- Loop Current: 20 mA

Changing the IP scheme on the ELAN

When changing the IP scheme of all the components of the CS 1000, maintain the order below:

1. Call server - LD 117
2. Gateway Controllers - use mgcsetup command to change the ELAN. Use Element Manager to change the TLAN. Refer to *Avaya Media Gateway 1000E PRI Gateway Installation and Commissioning, NN43041-311*.
3. COTS server - use Install menu in CD
4. MC32 and MC32s - refer to *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*.

Accessing the system

Logging in and out

When you access the system through a system terminal, a login procedure is required (refer to Logging in and out on page 28). All system passwords are initially set as 0000, but you can change passwords through the Configuration Record (LD 17). See also "Limited Access to Overlays" in the *Avaya Features and Services, NN43001-106*.

- Level 1 password. This general password is used in the log in sequence to provide general access to the system by service personnel. Once the system is accessed, the service personnel may then perform any necessary administration or maintenance tasks.
- Level 2 password. This administrative password is known and used only by the data administration manager. The password is used to protect the system configuration record and is required when using LD 17 to change either the general or the administrative passwords.

Local and remote access

Input/output terminals may operate either locally or remotely. However, data modems are required for terminals located more than 50 feet (15 meters) from the central control interface. Both local and remote terminals interface with the system through Serial Data Interface (SDI) cards.

Many devices can be installed at local and remote locations. When a system terminal is installed locally, it is connected directly to a SDI Card. When a system terminal is installed at a remote location, modems (or data sets) and a telephone line are required between the terminal and the SDI card. Figure 1: Local and remote access to a system terminal on page 27 shows typical system terminal configurations.

Multiple devices can simultaneously communicate with the system if Multi User Login is enabled. Refer to *Avaya System Management Reference, NN43001-600* for details regarding the Multi User Login Feature.

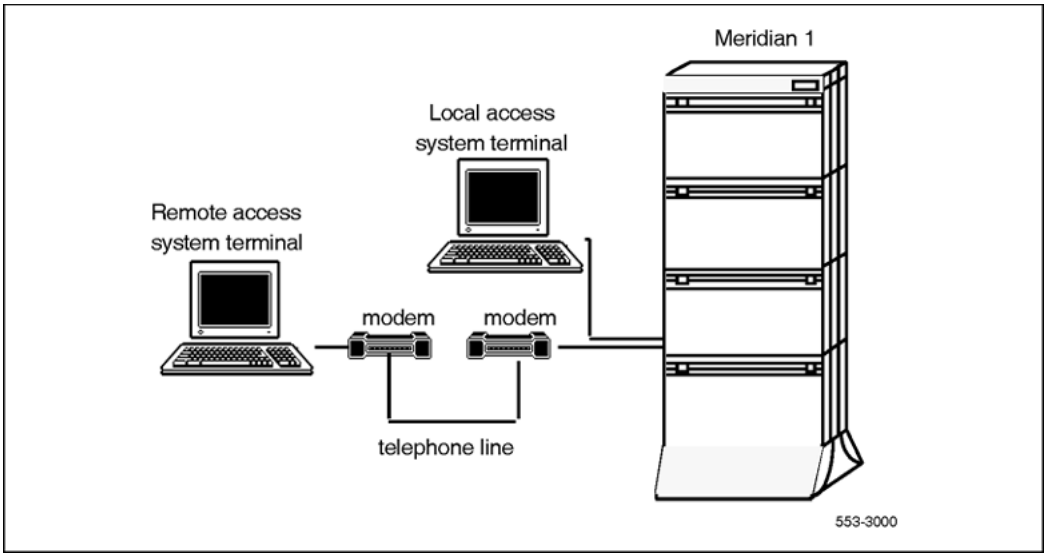


Figure 1: Local and remote access to a system terminal

HOST mode access

A system terminal is connected through an SDI port. SDI ports are defined in LD 17 and may be configured for different types of outputs. For example, one terminal may be defined for traffic reports, another for maintenance messages. Two ports may be defined for the same output.

It is possible to log in as a HOST. When in the HOST mode, the outputs defined for the port are only output to that port. This is useful for applications, which require high speed ports. Once the HOST port has logged out, the outputs to the other ports are restored.

To configure a system terminal, see the "System and limited access passwords" in the configuration record (LD 17). See also OVL403 and OVL404 messages, which are output to the ports affected by a HOST log in.

Line mode interface log in procedure

Line Mode interface gives the ability to edit entries made on the command line. With Line Mode enabled (LON), the backspace can be used to edit input. The entered information (responses, for example) is not processed until the <CR> is entered. When the Line Mode is disabled (LOF), the system terminal interface does not allow correction on the command line.

Note:
Line Mode interface requires the setting: seven data bits, space parity and one stop bit.

The Serial Data Interface (SDI) application on the Multi-Purpose Serial Data Link (MSDL) card offers the Line Mode Editing (LME) function. With the LME function enabled (FUNC=LME), the

backspace can be used to edit input. The LME function is only supported on VT200 type terminals running EM200 emulation mode.

Logging in and out

1. Press <CR>
    a. If the response is: `OVL111 nn TTY` or `OVL111 nn SL-1` That means: Someone else is logged into the system. When they have logged off, press <CR> and go to Step 2.
    b. If the response is: `OVL111 nn IDLE` or `OVL111 nn BACKGROUND` That means: You are ready to log into the system. Go to Step 2.
    c. If the response is: `OVL000 >`

    That means: This is the program identifier which indicates that you are have already logged into the system. Go to Step 4.
2. Enter: **`LOGI`**, then press `<CR>`

    The normal response is: `PASS ?`

    If there is any other response, refer to the message text in the System Error Messages document.
3. Enter: Level 1 or Level 2 password and press <CR>.

    If the password is correct, the system responds with the prompt: >
4. Load a program by entering: **`LD XXX`**(where XXX represents the overlay program number).
5. Perform tasks
6. End the program by entering: **`END`** or ****
7. Always end the log in session with: LOGO

    The background routines are then loaded automatically.

Access through the maintenance telephone

A telephone functions as a maintenance telephone when you define the class-of-service as MTA (maintenance telephone allowed) in the Multi-line Telephone Administration program (LD 11). A maintenance telephone allows you to send commands to the system, but you can only use a subset of the commands that can be entered from a system terminal.

You can test tones and outpulsing through the maintenance telephone. Specific commands for those tests are given in the Tone and Digit Switch and Digitone Receiver Diagnostic (LD 34).

To access the system using the maintenance telephone, see Procedure 2. To enter commands, press the keys that correspond to the letters and numbers of the command (for example, to

enter LD 42 return, key in 53#42##). Table 2: Translation from keyboard to dial pad on page 29 shows the translation from a keyboard to a dial pad.

The following overlays (LDs) ARE accessible from a maintenance telephone: 30, 32, 33, 34, 36, 37, 38, 42, 43, 45, 46, 60, 61, and 62

The following overlays (LDs) ARE NOT accessible from a maintenance telephone: 31, 40, 48, 77, 80, 92, 96, 135, 137

Note:
To use the maintenance telephone, the loop for that telephone must be operating.

Table 2: Translation from keyboard to dial pad

Keyboard				Dial pad
			1	1
A	B	C	2	2
D	E	F	3	3
G	H	I	4	4
J	K	L	5	5
M	N	O	6	6
P,Q	R	S	7	7
T	U	V	8	8
W	X	Y,Z	9	9
			0	0
			Space or #	#
			Return	##
			*	*

Note:
There is no equivalent for Q or Z on a dial pad.

Accessing through the maintenance telephone

1. Press the prime DN key.
2. Place the set in maintenance mode by entering: **`xxxx91`**

   Where: "xxxx" is the customer Special Prefix (SPRE) number. It is defined in the Customer Data Block and can be printed using LD 21. The SPRE number is typically "1" (which means you would enter 191).
3. Check for busy tone by entering "return": ##

a. If there is no busy tone, go to Step 4.

b. If there is a busy tone, a program is active. To end an active program and access the system enter: ****

4. Load a program by entering: **53#xx##**

   "xx" represents the number of the overlay program

5. Perform tasks.

6. To exit the program and return the telephone to call processing mode, enter: ****

   Background routines are then loaded automatically.

Accessing Meridian Mail

Small Systems allow access to Meridian Mail Administration & Maintenance through a shared terminal. To access the Meridian Mail system, log in and enter: AX. To exit from Meridian Mail, press the Control key and the closed square bracket ( ]) simultaneously.

System memory and disk space

The following memory information is output when an administration program is loaded. This information is used to plan the addition of new features, such as speed call lists, which require memory and disk space.

MEM AVAIL: (U/P): pppppp USED: qqqqqq TOT: rrrrr

or (depending on the total amount of memory)

MEM AVAIL: (U-ppppp1 P-ppppp2): USED: qqqqqq TOT: rrrrr

DISK RECS AVAIL: xxxxx, for Small Systems

DISK SPACE NEEDED: nnnnn KBYTES, for Large Systems

Legend:

Element	Definition
ppppp1	Amount of unprotected memory available for use (in words)
ppppp2	Amount of protected memory available for use (in words)
ppppp	Total memory available for use (ppppp1 + ppppp2) (in words)
qqqqq	Total amount of memory used (in words)

Element	Definition
rrrrrr	Total amount of memory (in words)
xxxxx	Records available for storage of additional data (Small Systems)
nnnnn	Records available for storage of additional data (Large Systems)

Low memory and disk warnings

If the amount of memory or disk space is low, the following messages are output on the systems.

WARNING: LOW MEMORY WARNING: LOW DISK WARNING: LOW MEMORY/DISK

Note:

The LOW DISK messages will not be displayed after sysload until a data dump is performed.

Warning:

When the LOW MEMORY, LOW DISK, or LOW MEMORY/DISK messages appear, avoid performing further administration changes which require more memory and disk space. These changes may be lost during the next data dump.

When low memory or disk problems occur, a review of system memory is recommended. Memory may be reclaimed by removing unused features. For example, the system may have speed call lists which are no longer used and can be removed.

Depending on the data storage type required (e.g., protected/ unprotected), it may be necessary to perform an initialize or sysload to access the reclaimed data store space.

A disk record stores approximately 500 words of protected data store. A single 3.5 inch high density floppy disk can hold a maximum of 1425 records.

When the software detects that more than one floppy disk is required, the data will be compressed during the backup, thereby reducing the number of disks required.

System Look up messages

On systems equipped with System Errors and Events Lookup package 245, it is possible to display system messages on screen. System messages must first be loaded into the switch by entering ERR <CR>. Specific system messages may then be viewed on screen if the user

enters the desired system error code and <CR>. The following example shows the data entries necessary to view error message SCH946:

- Login to switch
- PASS(Enter only your password)
- ERR <CR>(The user must type "ERR" and press return)
- SCH946 <<CR>(The user must type "SCH946" and press return)

The screen will now display the error message corresponding to SCH946. In this case, that message is:

```
Invalid User Type
```

For further information on system messages refer to the *Avaya Software Input Output Reference - System Messages, NN43001-712*.

Multi-User Login

Meridian 1 Multi-User Login (MULTI_USER) (package 242) enables up to five users to log in, load, and execute overlays simultaneously. These three users are in addition to an attendant console or maintenance terminal. The multi-user capability increases the efficiency of crafts persons by enabling them to perform tasks in parallel. To facilitate this operating environment, Multi-User Login includes significant functionality:

- Database conflict prevention
- Additional user commands
- TTY log files
- TTY directed I/O

For further information refer to the Overlay Loader and Multi-User Login section in this Guide.

User commands

User commands are available at the > prompt (after login but with no overlay executing), or from within an overlay. To issue a command from within an overlay, precede the command with an exclamation point (!).

For example, to issue the WHO command from within an overlay, type:

!WHO

For more information on User commands, refer to the Overlay Loader and Multi-User Login section in this guide.

Maintenance display codes

Maintenance displays are located on the faceplate of certain circuit cards. A maintenance display code is a one-, two-, or three-digit alphanumeric code which can indicate the status of the system and identify faulty equipment. For a detailed definition of these codes, see the section titled "HEX" in the System Error Messages document.

Time and date of fault

The system identifies the time that faults are detected. When a diagnostic message is output, a timestamp is output within 15 minutes. The format is:

```
TIMxxx  hh:mm dd/mm/yy CPU x
```

xxx is the system ID

The time, date, and system ID are set in LD 2.

Applications that use SFTP

The SSH File Transfer Protocol (SFTP) is a network protocol that provides confidentiality and integrity to the data (such as files or commands) transmitted between an SFTP client and a server. SFTP also allows a client and a server to authenticate each other using passwords.

The following applications used FTP prior to CS 1000 Release 6.0, but use SFTP in Release 6.0 and later:

- From CS to all devices
  - Account DB
  - Banner
  - SYSCFG.DB
- CS Redundancy: PSDL file update (applicable to Call Server Redundancy only)
- Other devices
  - MGC DB files transfer from CS
  - ITG OMM (Operation Measure Module) file transfer
  - Personal Directory

- PDT disk/file command transfer
- ITG log file, UMS transfer
- ITG commands, boot file, configuration, F/W, SNMP
- MGC, MC32S bootfile, configuration, loadware, installation file transfer
- IP phone F/W file transfer
- EM patching handler
- Manufacturing delivery patch distribution

Chapter 5: Alphabetical list of packages

The following list is a comprehensive alphabetical list of packages that can be equipped on your system.

Mnemonic	Feature Name	Number	Release
AA	Attendant Administration	54	1
AAA	Attendant Alternative Answering	174	15
AAB	Automatic Answerback	47	1
ABCD	16-Button Digitone/Multifrequency Telephone	144	14
ACDA	Automatic Call Distribution, Package A	45	1
ACDB	Automatic Call Distribution, Package B	41	1
ACDC	Automatic Call Distribution Package C	42	1
ACDD	Automatic Call Distribution Package D	50	2
ACDE	ACD/DN Expansion	388	25.4
ACLI	Analog Calling Line Identification	349	24
ACNT	Automatic Call Distribution, Account Code	155	13
ACRL	AC15 Recall	236	20
ADMINSET	Set Based Administration	256	21
ADSP	ACD Night Call Forward without Disconnect Supervision	289	23
AFNA	Attendant Forward No Answer	134	14
AINS	Automatic Installation	200	16
ALRM_FILTER	Alarm Filtering	243	19
ANI	Automatic Number Identification	12	1
ANIR	ANI Route Selection	13	1
AOP	Attendant Overflow Position	56	1
APL	Auxiliary Processor Link	109	10
ARDL	Automatic Redial	304	22
ARFW	Attendant Remote Call Forward	253	20
ARIE	Aries Digital Sets	170	14

Mnemonic	Feature Name	Number	Release
ATAN	Attendant Announcement	384	25.4
ATM	Automatic Trunk Maintenance	84	7
ATX	Autodial Tandem Transfer	258	20
AUXS	Automatic Call Distribution Package D, Auxiliary Security	114	12
AWU	Automatic Wake-Up	102	10
BACD	Basic Automatic Call Distribution	40	1
BARS	Basic Alternate Route Selection	57	1
BASIC	Basic Call Processing	0	1
BAUT	Basic Authorization Code	25	1
BGD	Background Terminal	99	10
BKI	Attendant Break-In/Trunk Offer	127	1
BNE	Business Network Expansion	367	25
BQUE	Basic Queuing	28	1
BRI	Basic Rate Interface	216	18
BRIL	BRI line application	235	18
BRIT	ISDN BRI Trunk Access	233	18
BRTE	Basic Routing	14	1
BTD	Busy Tone Detection Tone	294	21
CAB	Charge Account/Authorization Code	24	1
CALL ID	Call ID (for AML applications)	247	19
CASM	Centralized Attendant Services (Main)	26	1
CASR	Centralized Attendant Services (Remote)	27	1
CBC	Call-by-Call Service	117	13
CCB	Collect Call Blocking	290	21
CCDR	Calling line Identification in Call Detail Recording	118	13
CCOS	Controlled Class Of Service	81	7
CDP	Coordinated Dialing Plan	59	1
CDR	Call Detail Recording	4	1
CDRE	Call Detail Recording Expansion (7 digit)	151	13
CDRQ	ACD CDR Queue Record	83	3
CDRX	Call Detail Recording Enhancement	259	20

Mnemonic	Feature Name	Number	Release
CHG	Charge Account for CDR	23	1
CHINA	China Attendant Monitor Package	285	21
CHTL	China Toll Package	292	21
CISMFS	Commonwealth of Independent States Multifrequency Shuttle Signalling	326	23
CIST	Commonwealth of Independent States - Trunk	221	21
CNAME	Calling Name Delivery	333	23
CNUMB	Calling Number Delivery	332	23
COOP	Console Operations	169	14
CORENET	Core Network Module	299	21
CDIR	Corporate Directory	381	25
CPCI	Called Party Control on Internal Calls	310	22
CPGS	Console Presentation Group	172	15
CPIO	Call Processor Input/Output (Option 81C)	298	21
CPND	Calling Party Name Display	95	10
CPP	Calling Party Privacy	301	21
CPP_CNI	CP Pentium Backplane for Intel Machine	368	25
CPRK	Call Park	33	2
CPRKNET	Call Park Networkwide	306	22
CSL	Command Status Link	77	8
CTY	Call Detail Recording on Teletype Terminal	5	1
CUST	Multiple-Customer Operation	2	1
CWNT	Call Waiting Notification (Meridian 911)	225	19
DASS2	Digital Access Signaling System 2	124	16
DBA	Data Buffering and Access	351	24
DCON	M2250 Attendant Console	140	15
DCP	Directed Call Pickup	115	12
DDSP	Digit Display	19	1
DHLD	Deluxe Hold	71	4
DI	Dial Intercom	21	1
DISA	Direct Inward System Access	22	1
DKS	Digit Key Signaling	180	1

Mnemonic	Feature Name	Number	Release
DLDN	Departmental Listed Directory Number	76	5
DLT2	M2317 Digital Sets	91	9
DMWI	DPNSSI Message Waiting Indication	325	23
DNDG	Do-Not-Disturb, Group	16	1
DNDI	Do-Not-Disturb, Individual	9	1
DNIS	Dialed Number Identification System	98	10
DNWK	DPNSS Network Services	231	16
DNXP	Directory Number Expansion (7 Digit)	150	13
DPNA	Direct Private Network Access	250	21
DPNSS189I	Enhanced DPNSS1 Gateway	284	20
DPNSS	Digital Private Network Signaling System 1	123	16
DPNSS_ES	DPNSS Enhanced Services	288	21
DRNG	Distinctive Ringing	74	4/9
DSET	M2000 Digital Sets	88	7
DTI2	2 Mbit Digital Trunk Interface	129	10
DTD	Dial Tone Detector	138	10
DTOT	DID to Tie (Japan only)	176	16
EAR	Enhanced ACD Routing	214	17
ECCS	Enhanced Controlled Class of Service	173	15
ECT	Enhanced Call Trace	215	18
EDRG	Executive Distinctive Ringing	185	16
EES	End-To-End Signaling	10	1
EMUS	Enhanced Music	119	12
ENS	Enhanced Night Service	133	20
EOVF	ACD Enhanced Overflow	178	15
ESA	Emergency Services Access	329	23
ESA_CLMP	Emergency Services Access Calling Number Mapping	331	23
ESA_SUPP	Emergency Services Access Supplementary	330	23
ETSI_SS	Euro Supplementary service	323	22
EURO	Euro ISDN	261	20

Mnemonic	Feature Name	Number	Release
Extended MGP Resources	Extended Media Gateway PRI Resources	418	5.5
FAXS	HiMail Fax Server	195	18
FCC 68	FCC Compliance for DID Answer Supervision	223	17
FCA	Forced Charge Account	52	1
FCBQ	Flexible Call Back Queuing	61	1
FCDR	New Format CDR	234	18
FDID	Flexible DID	362	24
FFC	Flexible Feature Codes	139	15
FFCSF	Boss Secretary Filtering (FFC activation)	198	15
FGD	Feature Group D	158	17
FIBN	Fiber Network	365	25
FMCL	Converged Mobile Users	414	5.5
FNP	Flexible Numbering Plan	160	14
FRTA	French Type Approval	197	15
FTC	Flexible Tones and Cadences	125	16
FTDS	Fast Tone and Digit Switch	87	7
FXS	Flexible Services Package	152	25
GCM	General Call Monitor	344	24
GPRI	International 1.5/2.0 Mb/s Gateway	167	18
GRP	Group Call	48	1
GRPRIM	Geographic Redundancy Primary system	404	4.0
GRSEC	Geographic Redundancy Secondary system	405	4.0
GCM	Global Call Monitoring	344	24
H323_VTRK	H323 Virtual Trunk	399	3.0
HA	High Availability	410	5.0
HIST	History File	55	1
HOSP	Hospitality Management	166	16
HOT	Enhanced Hot Line	70	4/10
HSE	Hospitality Screen Enhancement	208	17
HVS	Meridian Hospitality Voice Service	179	16

Mnemonic	Feature Name	Number	Release
IAP3P	Integrated Services Digital Network Application Module Link for Third Party Vendors	153	13
ICDR	Internal CDR	108	10
ICON_PACKAGE	M3900 Full Icon Support	397	3.0
ICP	Intercept Computer Interface	143	10
IDA	Integrated Digital Access	122	16
IDC	Incoming DID Digit Conversion	113	12
IEC	Inter-Exchange Carrier	149	13
IMS	Integrated Message System UST and UMG are part of IMS Package.	35	2
INBD	International nB+D	255	20
INTR	Intercept Treatment	11	1
IPEX	IP Expansion	295	25
IPMG	IP Media Gateway	403	4.0
IPRA	International Primary Rate Access	202	15
ISDN	Integrated Services Digital Network	145	13
ISDN INTL SUP	ISDN Supplementary Features	161	14
ISL	ISDN signaling Link	147	13
ISPC	ISDN Semi-Permanent Connection	313	22
IVR	Hold in Queue for IVR	218	18
JDMI	Japan Digital Multiplex Interface	136	14
JPN	Japan Central Office Trunks	97	9
JTDS	Japan Tone and Digit Switch	171	14
JTTC	Japan Telecommunication Technology Committee	335	23
KD3	Spanish KD3 DID/DOD interface	252	20
L1MF	X08 to X11 Gateway	188	15
LAPW	Limited Access to Overlays	164	16
LLC	Line Load Control	105	10
LMAN	Automatic Call Distribution Load Management (C2)	43	1
LNK	ACDD, Auxiliary Link Processor	51	2
LNR	Last Number Redial	90	8

Mnemonic	Feature Name	Number	Release
LOCX	Location Code Expansion	400	4.0
LSCM	Local Steering Code Modifications	137	10
LSEL	Automatic Line Selection	72	4
M3900_PROD_ENH	M3900 Phase III Productivity Enhancement	386	25.4
M3900_RGA_PROG	M3900 Ring Again	396	3.0
M911 ENH	M911 Enhancement Display	249	25
MAID	Maid Identification	210	17
MASTER	Euro ISDN Trunk - Network Side	309	22
MAT	MAT 5.0	296	22
MC32	Meridian Companion Enhanced Capacity	350	24
MCBQ	Network callback Queuing	38	2
MCMO	Meridian 1 Companion Option	240	19
MCT	Malicious Call Trace	107	10
MED_LANG	M3904 Mediterranean Language group	395	3.0
MEET	MCDN End to End Transparency	348	24
MFC	Multifrequency Compelled Signaling	128	9
MFE	Multifrequency Signaling for Socotel	135	10
MINT	Message Intercept	163	15
MLIO	Multi-Language I/O Package	211	16
MLM	Meridian Link Modular Server	209	16
MLMS: Brazilian	Brazilian	264	20
MLMS: Chinese (PRC)	Chinese (PRC)	265	20
MLMS: Chinese (ROC)	Chinese (ROC)	266	20
MLMS: Dainish	Dainish	267	20
MLMS: Dutch	Dutch	268	20
MLMS: Finnish	Finnish	269	20
MLMS: Canadian French	Canadian French	270	20
MLMS: European French	European French	271	20
MLMS: German	German	272	20
MLMS: Italian	Italian	273	20

Mnemonic	Feature Name	Number	Release
MLMS: Japanese	Japanese	274	20
MLMS: Korean	Korean	275	20
MLMS: Norwegian	Norwegian	276	20
MLMS: Russian	Russian	277	20
MLMS: European Spanish	European Spanish	278	20
MLMS: Latin Am. Spanish	Latin American Spanish	279	20
MLMS: Swedish	Swedish	280	20
MLWU	Multi-Language Wake Up	206	16
MOBX	Mobile Extensions	412	5.5
MPH	Meridian 1 Packet Handler	248	19
MPO	Multi-Party Operations	141	20
MQA	Multiple Queue Assignment	297	21
MR	PPM/Message Registration	101	10
MSB	Make Set Busy	17	1
MSDL	Multipurpose Serial Data Link	222	18
MSDL SDI	MSDL Serial Data Interface	227	19
MSDL STA	MSDL Single Terminal Access	228	19
MSMN	Mobility Networking	370	25
MULTI_USER	Multi-User Login	242	19
MUS	Music	44	1
MUSBRD	Music Broadcast	328	23
MWC	Message Waiting Center	46	1
MWI	Message Waiting Indication Interworking with DMS	219	19
M911	Meridian 911	224	19
NACD	Network Automatic Call Distribution	207	15
NARS	Network Alternate Route Selection	58	1
NAS	Network Attendant Service	159	20
NAUT	Network Authorization Code	63	1
NCOS	Network Class Of Service	32	1

Mnemonic	Feature Name	Number	Release
NFCR	New Flexible Code Restriction	49	2
NGCC	Symposium Call Center	311	22
NGEN	Next Generation Connectivity	324	22
NI2	North America National ISDN Class II Equipment	291	21
NI-2 CBC	NI-2 Call By Call Service Selection	334	23
NI-2 Name	NI-2 Name Display Supplementary Service	385	25.4
NMCE	NGenR2/Meridian Communication Exchange Connectivity	364	24
NMS	Network Message Services	175	16
NSC	Network Speed Call	39	2
NSIG	Network Signaling	37	2
NTRF	Network Traffic Measurements	29	1
NTWK	Advanced ISDN Network Services	148	13
NXFR	Network Call Transfer	67	3
OAS	Observe Agent Security	394	3.0
ODAS	Office Data Administration System	20	1
OHOL	On Hold On Loudspeaker	196	20
OHQ	Off-Hook Queuing	62	1
OOD	Optional Outpulsing Delay	79	5
OPAO	Outpulsing, asterisk (*) and octothorpe (#)	104	
OPCB	Operator Call Back (China #1)	126	14
OPEN ALARM	Open Alarms	315	22
OPTF	Optional Features	1	1
ORC_RVQ	Remote Virtual Queueing	192	18
OVLP	Overlap Signaling (M1 to M1 and M1 to 1TR6 CO)	184	15
PAGENET	Call Page Networkwide	307	22
PAGT	Automatic Call Distribution, Priority Agent	116	12
PBXI	1.5 Mbit Digital Trunk Interface	75	5
PCA	Personal Call Assistant	398	3.0
PEMD	Pulsed E&M (Indonesia, French Colise)	232	18
PHTN	Phantom TN	254	20
PLDN	Group Hunt/DN Access to SCL	120	15

Mnemonic	Feature Name	Number	Release
PLUGIN	Plug-In	366	24
PMSI	Property Management System Interface	103	10
PONW	Priority Network Override	389	25.4
POVR	Priority Override/Forced Camp-On	186	20
PQUE	Network Priority Queuing	60	1
PRA	Primary Rate Access (CO)	146	13
PRI2	2.0 Mb/s Primary Rate Interface	154	14
PVQM	Proactive Voice Quality Management	401	4.0
PXLT	Pretranslation	92	8
QSIG	Q reference signaling point Interface	263	20
QSIG GF	QSIG Generic Functional protocol	305	22
QSIG SS	QSIG Supplementary service	316	22
RAN	Recorded Announcement	7	1
RANBRD	Recorded Announcement Broadcast	327	23
RCK	Ringing Change Key	193	15
REMOTE_IPE	Remote IPE	286	
RMS	Room Status	100	10
ROA	Recorded Overflow Announcement	36	2
RPA	Radio Paging	187	15
RUCM	Russian Call Monitoring	353	24
RVQ	Remote Virtual Queuing	192	18
SACP	Semi-Automatic Camp-On	181	15
SAMM	Stand-alone Meridian Mail	262	20
SAR	Scheduled Access Restrictions	162	20
SBO	Branch Office	390	2.0
SCC	Tone Detector Special Common Carrier	66	7
SCDR	Station Activity Records	251	20
SCI	Station Category Indication	80	7
SCMP	Station Camp-On	121	20
SECL	Series Call	191	15
SIP	SIP Gateway and Converged Desktop	406	4.0

Mnemonic	Feature Name	Number	Release
SIPL_AVAYA	Avaya SIP Lines	415	5.5
SIPL_3RDPARTY	Third Party SIP Lines	416	5.5
SLP	Station Loop Preemption	106	10
SMS	Short Message Service	346	24
SNR	Stored Number Redial	64	3
SOFTSWITCH	Soft Switch	402	4.0
SR	Set Relocation	53	1
SSAU	Station Specific Authorization Codes	229	19
SS5	500 Set Dial Access to Features	73	4
SS25	2500 Set Features	18	1
SSC	System Speed Call	34	2
STA	Single Term Access	228	19
STS	Set to Set Messaging	380	25
SUPP	International Supplementary Features	131	9
SUPV	Supervisory Attendant Console	93	8
SVCT	Supervisory Console Tones	189	20
SYS_MSG_LKUP	System Errors and Events Lookup	245	19
TAD	Time and Date	8	1
TATO	Trunk AntiTromboning	312	
TBAR	Trunk Barring	132	20
TDET	Tone Detector	65	7
TENS	Multiple-Tenant Service	86	7
TFM	Trunk Failure Monitor	182	15
THF	Trunk Hook Flash (Centrex)	157	14
TLSV	Telephony Services	413	5.5
TMON	Traffic Monitoring	168	
TOF	Automatic Call Distribution, Timed Overflow Queuing	111	10
TSET	M3000 Digital Sets	89	7
TVS	Trunk Verification from Station	110	9.32
TWR1	Taiwan R1	347	24
UIGW	Universal ISDN Gateways	283	20

Mnemonic	Feature Name	Number	Release
UK	United Kingdom	190	16
UUI	Call Center Transfer Connect	393	3.0
VAWU	VIP Auto Wake Up	212	17
VMBA	Voice Mailbox Administration	246	19
VIR_OFF_ENH	M3900 Phase III Virtual Office Enhancement	387	25.4
VIRTUAL_OFFICE	Virtual Office	382	25
VNS	Virtual Network Services	183	16
VO	Virtual Office	382	3.0
VOE	Virtual Office Enhancement	387	3.0
XCT0	M1 Enhanced Conference, TDS and MFS	204	15
XCT1	M1 Superloop Administration (LD 97)	205	15
XPE	Meridian 1 XPE	203	15
ZCAC	Zone Call Admission Control	407	4.50

Chapter 6: Overlay loader and Multi-User Login

Overlay loader

The Overlay loader becomes active after the login sequence and password, it will then accept input commands from the Serial Data Interface Terminals (SDI) after the ">" prompt (after login but with no overlay executing).

Overlay loader commands

The Overlay loader commands are as follows:

Command	Description
ERR	Display the last error message given. Only available on systems with System Errors and Events Lookup package 245 equipped.
ERR x..x	Specific system messages are displayed (package 245 required). Where: x..x = specific error type and number (ex. ERR SCH1001)
FDLC	Cancel or stop system wide flash download for M39xx units.
LD xxx	Load overlay program into the overlay area, then the loaded program assumes control. Where: xxx = number of the desired overlay program.
LOF	Disable Line Mode interface (TTY setup: 7 data bits, space parity, 1 stop bit).
LOGO	Exit overlay loader and Log-off the system.
LON	Enable Line Mode interface (TTY setup: 7 data bits, space parity, 1 stop bit).
****	Aborts the current overlay program, allowing another overlay program to be loaded into the overlay area.

Multi-User Login commands

Multi-User Login enables up to five users to log in, load, and execute overlay programs simultaneously. These three users are in addition to an attendant console or maintenane terminal. The Multi-User capability also introduces several user commands. With these commands, the user has the ability to:

- determine who is logged into the system
- communicate with other connected users
- halt and resume background and midnight routines
- initiate and terminate terminal monitoring
- change printer output assignment

Note:
MULTI_USER must be enabled in LD 17.

With multiple overlays operating concurrently, there is the potential for a database conflict if two or more overlays attempt to modify the same data structure. Multi-User Login software prevents such conflicts. When a user requests that an overlay be loaded, the software determines if it could pose a potential conflict with an overlay that is already executing. If no conflict exists, the requested overlay is loaded. If a conflict does exist, the system issues the following message:

OVL429-OVERLAY CONFLICT

The user can try again later, or try to load a different overlay.

For Release 6.5 and greater, the overlay conflict resolution check is relaxed to allow Multi User Overlays to operate concurrently with LD 43 if only the database backup is performed on the Overlay. For example, backup to removable storage media, CCBR or GR backup.

Multi-User commands

A user can issue any of the commands listed in the following table from Overlay loader or from any position within an overlay. Precede the command with an exclamation point (!) to issue a command from within an overlay.

For example, to issue the WHO command from within an overlay, type:

!

>WHO

> <CR> takes user back to the same position in current overlay

Command	Description
WHO	Displays user name, port ID, and overlay loaded for each logged-in terminal, as well as the user's MON and SPRT commands (see below).
SEND xx	Sends a message to logged-in terminal xx. When the system responds with a " SEND MSG: " prompt, enter the message text yy...yy (up to 80 characters). The text of a message is considered private and therefore is not written to any log file.
SEND ALL	Sends a message to all logged-in terminals. When the system responds with a " SEND MSG: " prompt, enter the message text yy...yy (up to 80 characters). The text of a message is considered private and therefore is not written to any log file.
SEND OFF	Prevents messages sent by other terminals from appearing at the user's terminal.
SEND ON	Enables messages sent by other terminals to appear at the user's terminal.
FORC xx	Forces terminal xx to log off (the requesting user must log in with LAPW or a level 2 password).
HALT	Stops background and midnight routines during a login session.
HALT OFF	Resumes halted background and midnight routines.
MON xx	Initiates monitoring for terminal xx (the requesting user must log in with LAPW or a level 2 password). The monitored terminal receives a message at the beginning and end of the monitored period.
MON OFF	Turns off the monitor function.
SPRT xx	Assigns printer output to port xx.
SPRT OFF	Resets printer output assignment.

Note:

For detailed information about Multi-user login, see *Avaya System Management Reference, NN43001-600*

Chapter 7: LD 01: Template audit

Templates are used to store data that is common to many telephones. This data includes items such as key functions and Class of Service. The Template Audit program saves protected memory by eliminating unused or duplicate telephone templates.

Consistency Checks

LD 1 also performs the following consistency checks.

User Count Scan

All telephones in the system are scanned to find the total number of users for a template.

If a template is found to have no users, the entire template is removed with the warning message 'NO USERS FOUND'. If a template is found to have an incorrect user count, the correct user count is written to the template, and the warning message 'USER COUNT LOW' or 'USER COUNT HIGH' is output. If the user count is accurate, the message 'USER COUNT OK' is output.

Duplicate Template Scan

Each template is checked against every other template for possible duplication. A template is considered a duplicate of another if all of the following conditions are met:

- the checksums are the same
- the template lengths and the hunt offsets are the same
- all template entries are the same

If a match is found, the warning message 'DUPLICATE OF xxxx' is output. A scan is then initiated to locate all users of the current template and move them to the matched template.

For each of these users found, the template number in the telephone data block and the user count is updated. After all of the users of the current template are moved to the matched template, the current template is removed.

Template Checksum Audit

A checksum is a binary sum of the template length, hunt offset, and template entries. The checksum is calculated for each template and compared with the existing template checksum. If the existing checksum is correct, the message 'CHECKSUM OK' is output. Otherwise, the checksum is corrected with the warning message 'CHECKSUM WRONG'.

Key Lamp Strip Audit

Two checks are made to correct Key Lamp Strip (KLS) corruption. First, the template length is compared to the number of KLS indicated in the protected line block. The second check verifies that the last word of the template reflects a 'NULL' key.

If these checks detect any discrepancies, they are corrected with the warning message 'CORRPTED KLS'.

These corrections alter the checksum of the template. This is identified and corrected by the checksum audit.

Template Pointer Audit

Telephone data blocks contain a pointer to the template block that they use. These pointers are checked to insure they are correct for the template number stored in the same block. Any errors are reported and corrected.

Following is an example of the system information which is generated during a Template Pointer Audit:

```
STARTING TEMPLATE POINTER SCAN
BAD SL1 TEMPLATE PTR CORRECTED   TEMPLATE 0006
```

Operating parameters

Due to the Real Time impact of this program and the large amount of data being scanned, the template audit should be run during low traffic hours.

The template audit should not be aborted unless it is critically necessary. If it does become necessary to interrupt execution of the audit, be aware that the templates may be corrupted.

If a system initialization occurs during the template audit, the program is automatically aborted. It should be restarted as soon as possible after this occurs.

The audit printout only appears on the TTY that requested the template audit program run.

Template Audit cannot be run as a background task.

To confirm that extraneous templates have been removed and that all counts have been corrected to their proper value, re-run the audit program.

A datadump (LD 43) should be run after a template audit is executed.

Sample operation

The audit begins when the program (LD 1) is loaded. All templates are scanned in the following sequence, beginning with template one:

1. Single line telephones
2. Multi-line telephones

Following is an example of the system information which is generated during a Template Audit:

```
TEMPLATE AUDIT
CONFIRM TEMPLATE AUDIT NOW? (Y/N) Y
STARTING PBX TEMPLATE SCAN
TEMPLATE AUDIT
STARTING PBX TEMPLATE SCAN
TEMPLATE 0001 USER COUNT LOW      CHECKSUM OK
TEMPLATE 0002 USER COUNT HIGH      CHECKSUM OK
TEMPLATE 0003 NO USERS FOUND
STARTING SLl TEMPLATE SCAN
TEMPLATE 0001 USER COUNT OK      CHECKSUM OK
TEMPLATE 0067 USER COUNT OK CHECKSUM WRONG
TEMPLATE 0068 USER COUNT OK CHECKSUM OK DUPLICATE
OF 0014
TEMPLATE 0082 USER COUNT OK CHECKSUM OK
TEMPLATE 0120 USER COUNT OK
TEMPLATE AUDIT COMPLETE
```

Note:
The report does not print out that template inconsistencies have been corrected.

Chapter 8: LD 30: Network and Signaling Diagnostic

This program is used to maintain Network loops. It can be run in background, loaded during the daily routines or loaded manually to enter commands.

Program operation

When invoked automatically by the system, the program performs the following tests:

- network memory of each enabled network card
- continuity of the speech path to each IPE shelf (for enabled loops only)
- signaling channel to each line or trunk card (on enabled loops only)
- signaling channel through each Integrated Services digital line card to each Digital telephone or data TN
- clock controllers are switched (if either DTI2 or PRI2 are used when LD 30 is run in midnight mode, clock controllers will not be switched)

For the Integrated Voice Messaging System (IVMS), the program does not test Automatic Call Distribution (ACD) positions when the positions belong to IVMS-DN groups.

Digital telephones that pass the signaling test have their date and time updated to match the system clock.

Any SL-1 telephone or card that fails the signaling test may be disabled by this program. Use LD 32 to re-enable them.

If two or more IPE cards are disabled on a loop, an NWS101 message is printed without the associated NWS301 messages to indicate card failures. However, the shelves that failed are known from the NWS201 messages. Therefore, the state of the individual cards can be determined by manually retesting using the SHLF command.

If NWS301 indicates a failure of the Peripheral Buffer or Controller card, the message may not be correct. Therefore the card should be retested using the SHLF command.

This program does not test attendant consoles. Equipment that has been disabled, due either to overload or manual request, is not tested.

On Small Systems and CS 1000S systems, a continuity test and signaling test on the IPE shelf is performed when LD 30 is invoked automatically.

How to use LD 30

When invoked manually on systems, the Overlay may be used to:

- conduct a complete test, as when the program is invoked automatically, except for switching the clocks
- conduct a test on a specific IPE shelf
- get the enable/disable status of network loops
- enable or disable network loops
- clear alarm indications and the maintenance display
- download peripheral software on superloops
- clear contents of the Controller maintenance display
- read contents of the Controller maintenance display

When invoked manually on a Small System, the program may be used to:

- conduct a complete test, as when the program is invoked automatically, except for switching the clocks
- clear alarm indications and the maintenance display
- perform a signaling test on a specific card or unit
- perform a continuity test and signaling test on the Small SystemIPE shelf

Fibre Network Fabric

The Fibre Network Fabric Expansion extends and enhances the 5-group network architecture to 8 non-blocking (inter-group) Network groups, with a resulting expansion in network capacity to 8k timeslots available for Intergroup traffic. This is achieved by using OC-12 SONET rings, and adding additional network and IPE shelves, cards and cables and software changes to allow using the expanded network capacity. This expansion increases the number of available loops from 160 to 256. This applies to Multi Group systems only.

Basic commands

Contents

Section
Large System and Avaya Communication Server 1000E commands on page 57
Small Systems, CS 1000S, MG 1000B, and MG 1000T commands
Superloop commands
Basic Rate Interface (BRI) commands
Small Systemand CS 1000S BRI commands

Large System and Avaya Communication Server 1000E commands

The following commands are applicable to all Large System and Avaya CS 1000E Systems:

CDSP	Clear the maintenance display on active CPU to 00 or blank
CMAJ	Clear major alarm and reset power fail transfer
CMIN	Clears minor alarm for all customers
CMIN ALL	Clears minor alarm for all customers
DISL loop	Disable loop
DISL sl	Disable specified superloop
END	Abort current test
ENLL loop	Enable network loop
ENLL sl	Enable specified superloop
LDIS	List disabled loops
LENL	List enabled loops

LOOP loop, ALL	Test network memory on one or all loops
SHLF l s	Test loop l, shelf s
STAT	Get status of all network loops
STAT loop	Get status of specified loops

Superloop commands

The following commands are used with Controllers (NT8D01) and Network Cards (NT8D04 or NT8D18):

CPED l s	Clear contents of Controller maintenance display on loop l shelf s
DISL loop	Disable loop
END	Abort current test
ENLL loop (v)	Enable superloop, download peripheral software version v
LDIS	List disabled loops
LENL	List enabled loops
LOOP loop, ALL	Test network memory on one or all loops
RPED l s	Read contents of the Controller maintenance display
SHLF l s	Test loop l, shelf s
STAT	Get status of all network loops
STAT (loop)	Get status of specified loop
UNTT l s c (u)	Do a signaling test on specified card or unit

Basic Rate Interface (BRI) commands

The following commands are used with Multi-purpose ISDN Signal Processor (MISP), S/T-Interface Line (SILC), and U-Interface Line (UILC) cards:

SLFT l s c	Invoke self-test on ISDN BRI line card

SLFT l s c type	Selftest ISDN BRI line card. The card must be disabled. Response is: NWS637 selftest passed or NWS632 selftest failed. Where: l = loop, s = shelf, c = card, and type = self-test type (Long or Short)

STEI l s c u	Query the Terminal Endpoint Identifiers, and their corresponding USIDs
	This command queries the TEIs, and their corresponding USIDs on the specified DSL with an established D-channel data link layer with the MISP. Output looks like:
	`MISP 111`
	`TEI  USID`
	`---  ----`
	`nnn  nnnn`

SLFT loop type	Invoke self-test on MISP loop. Where: type = 1 (comprehensive test) or type = 2 (power on reset)
TEIT l s c u	Perform TEI check on Digital Subscriber Loop, where: • l = (0-255) Multi Group systems with Fibre Network Fabric • u = 0-7

Alphabetical list of commands

Command	Description	Pack/Rel
CDSP	Clear the maintenance display on active CPU to 00 or blank.	basic-1
CMAJ	Clear major alarm, reset power fail transfer and clear power fault alarm.	basic-1
CMIN	Clears minor alarm for all customers	alrm_filter-22
CMIN ALL	Clears minor alarm for all customers	basic-1
CPED l s	Clear contents of Controller maintenance display on loop l shelf s, where: l = 0-252 and must be a superloop (multiple of 4), Multi Group systems with Fibre Network Fabric This also clears the buffer printed with the command RPED.	xpe-15 fnf-25

Command	Description	Pack/Rel
DISL loop	Disable loop. All calls in progress on this loop are disconnected. Peripheral cards remain software enabled and no LEDs are lit.	basic-1
DISL sl	Disable specified superloop. Active calls on the superloop specified will be disconnected and line transfer will occur at the remote end.	basic-21
END	Abort current test. If no test is in progress, message NWS002 is output.	basic-1
ENLL loop	Enable network loop. This enables the network, performs a network memory test and tests continuity and signaling to all shelves on the loop. If it passes the test, OK is output. This does not re-enable any disabled cards on the loop. Use LD 32 ENLS or ENXP commands or enable each card individually. When enabling a network loop serving ISDLC cards, the ISDLC cards must be individually disabled, then re-enabled to ensure that service is restored to digital telephones. Service may also be restored to digital telephones by disconnecting and then reconnecting the telephone's line cord.	basic-1
ENLL loop (v)	Enable superloop, download peripheral software version v. If version v is not specified, the software downloaded is current (c) or latest (l) version as defined in LD 97.	xpe-15
ENLL sl	Enable specified superloop. OK is output if superloop has been enabled. Establishing service of individual voice-and-data-capable carriers is dependant on the F/W state of that carrier.	basic-21
LDIS	List disabled loops, where:	basic-1
	loop = 0-255, Multi Group systems with Fibre Network Fabric	fnf-25
	Response is: `l1, l2, ln:` loop is a disabled loop, or `NONE:` If no cards are enabled.	
LENL	List enabled loops, where:	basic-1

Command	Description	Pack/Rel
	loop = 0-255, Multi Group systems with Fibre Network Fabric	fnf-25
	Response is: • `l1, l2, ln:` l is an enabled loop, or • `NONE:` if no cards are enabled	
LOOP loop, ALL		
	Performs a network memory test, continuity test and signaling test on all XOPS cards on specified loop. If ALL is specified, every loop currently enabled is tested. If no errors are detected, OK is output, where: loop = 0-159	basic- 20
	loop = 0-255, Multi Group systems with Fibre Network Fabric	fnf-25
	Out-of-Service units are not tested when this command is used.	
RPED l s	Read contents of the Controller maintenance display, where:	xpe-15
	l = 0-252 and must be a superloop (multiple of 4), Multi Group systems with Fibre Network Fabric	fnf-25
	This command lists the current and last 15 clock tracking states of the NT8D01 Controller. The tracking is indicated on the Controller maintenance display. The possible tracking modes are: • C0 = Controller is tracking to the network connected to port 0 • `C1` = Controller is tracking to the network connected to port 1 • `C2` = Controller is tracking to the network connected to port 2 • `C3` = Controller is tracking to the network connected to port 3 • `CF` = Controller is not tracking any network. See HEX messages for the interpretation of Controller maintenance display codes.	
SHLF l s	Test loop l, shelf s. Performs a network memory test, continuity test and signaling test only on loop l shelf s. All line cards, idle trunk	basic- 20

Command	Description	Pack/Rel
	cards, XOPS cards and idle SL-1 telephones are tested. If no errors are detected, OK is output. Out-of-service units are not tested when this command is used.	
	Performs a network memory test, continuity test and signalling test on loop 0-255 and shelf only for Multi Group systems with Fibre Network Fabric	fnf-25
SLFT card	Invoke self-test for ISDN BRI line card. The card must be disabled, where response is: • NWS632 self-test failed • NWS637 self-test passed (Small System)	bri-18
SLFT l s c	Invoke self-test for ISDN BRI line card. The card must be disabled.	bri-18
SLFT l s c type		rsc/bri-19
	Self-test ISDN BRI line card. The card must be disabled, where: • l = loop, 0-255, Multi Group systems with Fibre Network Fabric • s = shelf • c = card • type = self-test type (Long or Short) Response is: NWS637 selftest passed, or NWS632 selftest failed, where:	fnf-25
SLFT card type		bri-18
	Invoke self-test for MISP card on Small System. The comprehensive test is run automatically when the MISP is enabled. The card must be disabled, where: • cardtype = 1 (comprehensive) • cardtype = 2 (power-on-reset) Response is: • NWS632 self-test failed • NWS637 self-test passed	
SLFT loop type		bri-18
	Invoke self-test for MISP card, where:	fnf-25

Command	Description	Pack/Rel
	• l = 0-255, Multi Group systems with Fibre Network Fabric • type is: - 1 (comprehensive) - 2 (power-on-reset) The comprehensive test is run automatically when the MISP is enabled. The card must be disabled, where response is: • NWS632 self-test failed • NWS637 self-test passed	
STAT	Gives status of network loops (circuits), indicating how many are enabled and how many are disabled. Response is: `x ENBL, y DSBL`	basic-1
STAT loop	Get status of a network loop, where: l = 0-255, Multi Group systems with Fibre Network Fabric Response is one of the following: • `UNEQ` = loop is unequipped • `DSBL: RESPONDING` = loop is disabled and the Network card is responding. The loop may have been disabled because of: - DISL command - associated Peripheral Signaling (PS) card is disabled - overload condition on associated loop. In this case an OVD message is output. An attempt to enable the loop may result in a recurrence of the overload. • `DSBL: NOT RESPONDING` = loop is disabled and the Network card is not responding. The card is missing, disabled by the faceplate switch or is faulty. • `x BUSY, y DSBL` = loop is enabled with x channels busy, y channels disabled. • `CTYF l1, l2...` = loop specified in the STAT command cannot receive speech from one or more loops (l1, l2). This usually indicates the LD 30 continuity test failed. Probable fault is the network card.	basic-1 fnf-25
STEI l s c d	Query the Terminal Endpoint Identifiers, and their corresponding USIDs, where:	brsc-19

Command	Description	Pack/Rel
	l = 0-255, Multi Group systems with Fibre Network Fabric	fnf-25

	This command queries the TEIs, and their corresponding USIDs on the specified DSL with an established D-channel data link layer with the MISP. Output looks like:
	`MISP 111`
	`TEI USID`
	`--- ----`
	`nnn nnnn`	

TEIT c u	Perform TEI check on Digital Subscriber Loop on Small Systems, CS 1000S, MG 1000B, and MG 1000T, where: u = 0-7 This test is carried out on a single specified DSL interface. It checks the existence of the defined TEIs and any possible duplication of TEIs. Duplicate TEIs are removed by the layer 2 task on the MISP.	bri-18
TEIT l s c u	Perform TEI check on Digital Subscriber Loop, where:	bri-18
	• l = 0-255, Multi Group systems with Fibre Network Fabric	fnf-25
	• u = 0-7 This test is carried out on a single specified DSL interface. It checks the existence of the defined TEIs and any possible duplication of TEIs. Duplicate TEIs are removed by the layer 2 task on the MISP.	
TEST	Perform a continuity test and signaling test on Small Systems, CS 1000S, MG 1000B, and MG 1000T IPE shelf.	basic-1
UNTT c (u)	Do a signaling test on specified card or unit on Small Systems, CS 1000S, MG 1000B, or MG 1000T.	xpe- 20
UNTT l s c (u)	Do a signaling test on specified XOPS card or unit. This command applies only to superloops, where:	xpe- 20
	• l = 0-255, Multi Group systems with Fibre Network Fabric	fnf-25
	• u = 0-31, but only 0-7 are allowed on the XOPS card Out-of-service units are not tested when this command is used.	

Chapter 9: LD 31: Telephone and Attendant Console Diagnostic

This program tests the keys and lamps of telephone sets and attendant consoles. The tests consist of pressing keys on a telephone and checking for the correct response.

After loading the program, any telephone in the system may invoke the test by dialing SPRE 92, (SPRE is the Special Service Prefix Code for the customer). No further inputs from the TTY are needed. If commands are input, the system responds with TRM001 indicating an invalid command.

To start the test:

1. Load program 31.
2. Dial SPRE 92 from the telephone to be tested.
3. Perform the steps given in the appropriate Table. The expected responses for LCD lamps, displays and tones are given. Each key need only be operated momentarily.

The volume keys (VOL UP and VOL DOWN) have eight levels. The level is adjusted by operating a key once for a change in one level. These keys control the audible level for ring volume, buzz volume and speech/tone volume.

Note:
When enabling a network loop with ISDLC cards, the ISDLC cards must be individually disabled and then re-enabled to restore service to digital telephones. Service may also be restored to digital telephones by disconnecting then reconnecting the telephone's line cord.

M2006 and M2008 Telephone test

The M2006 and M2008 faceplate is shown in Figure 2: Meridian M2006 and M2008 set on page 66. The M2006 test is provided in Table 3: Meridian M2006 Telephone test on page 66. The M2008 test is provided in Table 4: Meridian M2008 Telephone test on page 67.

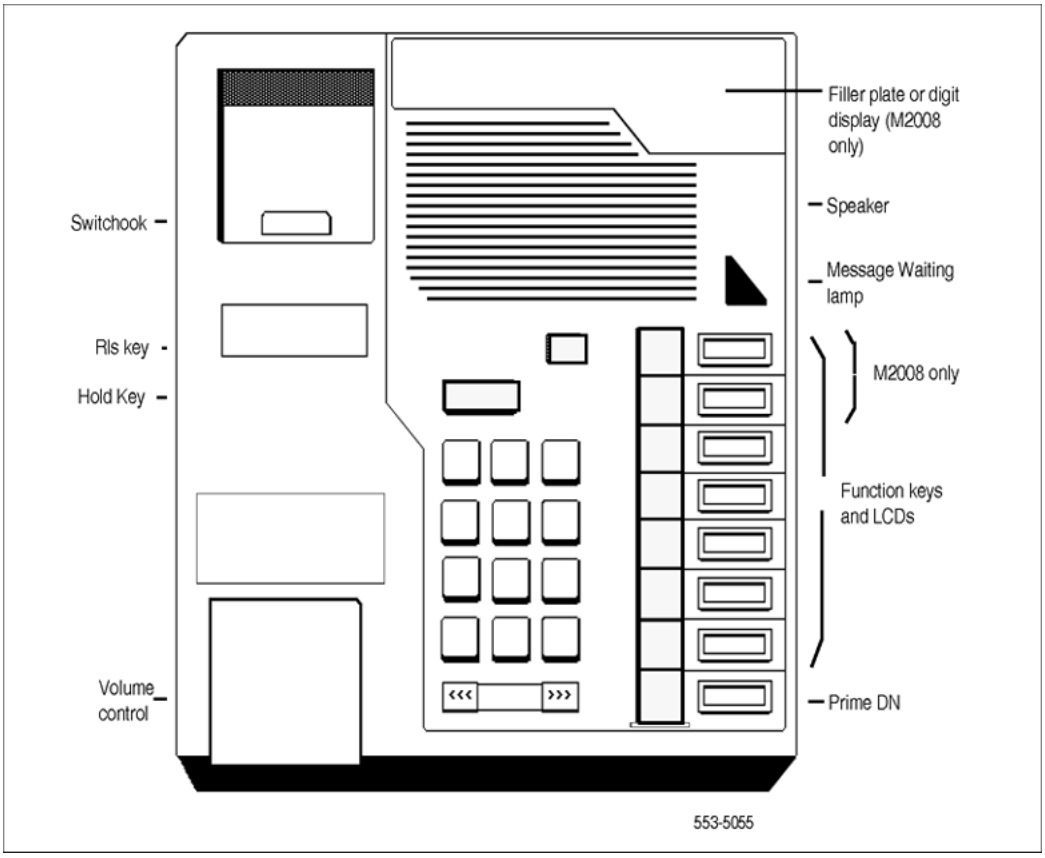


Figure 2: Meridian M2006 and M2008 set

Table 3: Meridian M2006 Telephone test

Step	Key operated	LCD location and response	Display and Tones
	Feature keys:		
1	Key 0	LCD 0 lit	
2	Key 1	LCD 1 lit	
3	Key 2	LCD 2 lit	
4	Key 3	LCD 3 lit	turn on Message Waiting LED
5	Key 4	LCD 4 lit	turn off Message Waiting LED
6	Key 5	LCD 5 lit, (if key 5 is not a Program key for data option)	
	Keypad keys:		
7	Key 1	LCD 0 lit	
8	Key 2	LCD 1 lit	
9	Key 3	LCD 2 lit	

Step	Key operated	LCD location and response	Display and Tones
10	Key 4	LCD 3 lit	
11	Key 5	LCD 4 lit	
12	Key 6	LCD 0 and 4 lit	
13	Key 7	LCD 1 and 4 lit	
14	Key 8	LCD 2 and 4 lit	
15	Key 9	LCD 3 and 4 lit	
16	Key 0	LCD 1 and 4 lit	
17	Key *	all LCDs lit	
18	Key #	all LCDs off	
	Fixed keys:		
19	HLD	LCD 0 to 4 lit	dial tone
20	Release	all LCDs off	
21	Off-hook	all LCDs flash	dial tone from handset only
22	On-hook	all LCDs fast flash	dial tone form speaker
23	Off-hook	all LCDs lit	
24	On-hook	all LCDs off	
25	HLD	LCD 0 to 4 lit	buzzer
26	HLD	end of test	

Table 4: Meridian M2008 Telephone test

Step	Key operated	LCD location and response	Display and Tones
	Feature keys:		
1	Key 0	LCD 0 lit	display upper case letters
2	Key 1	LCD 1 lit	display lower case letters
3	Key 2	LCD 2 lit	display clear
4	Key 3	LCD 3 lit	display darkens
5	Key 4	LCD 4 lit	top line of display darkens
6	Key 5	LCD 5 lit	turn Message Waiting LED on
7	Key 6	LCD 6 lit	turn Message Waiting LED off
8	Key 7	LCD 7 lit	
	Keypad keys:		

Step	Key operated	LCD location and response	Display and Tones
9	Key 1	LCD 0 lit	1 on display
10	Key 2	LCD 1 lit	2 on display
11	Key 3	LCD 2 lit	3 on display
12	Key 4	LCD 3 lit	4 on display
13	Key 5	LCD 4 lit	5 on display
14	Key 6	LCD 5 lit	6 on display
15	Key 7	LCD 6 lit	7 on display
16	Key 8	LCD 0 and 6 lit	8 on display
17	Key 9	LCD 1 and 6 lit	9 on display
18	Key 0	LCD 2 and 6 lit	0 on display
19	Key *	all LCDs lit	bottom line of display darkens
20	Key #	all LCDs off	display clear
	Fixed keys:		
21	HLD	LCD 0 to 4 lit	
22	Release	all LCDs off	display clear
23	Off-hook	all LCDs flash	dial tone from handset only
24	On-hook	all LCDs fast flash	dial tone form speaker
25	Off-hook	all LCDs lit	display darkens
26	On-hook	all LCDs off	display clear
27	HLD	LCD 0 to 4 lit	buzzer
28	HLD	end of test	

M2216, M2016S, and M2616 Telephone test

The set faceplate is shown in Figure 3: M2216, M2016S and M2616 set on page 69. The M2216 test is provided in Table 5: M2216 Telephone test on page 69. The M2016S and M2616 set test is provided in Table 6: M2016S and M2616 Telephone test on page 70.

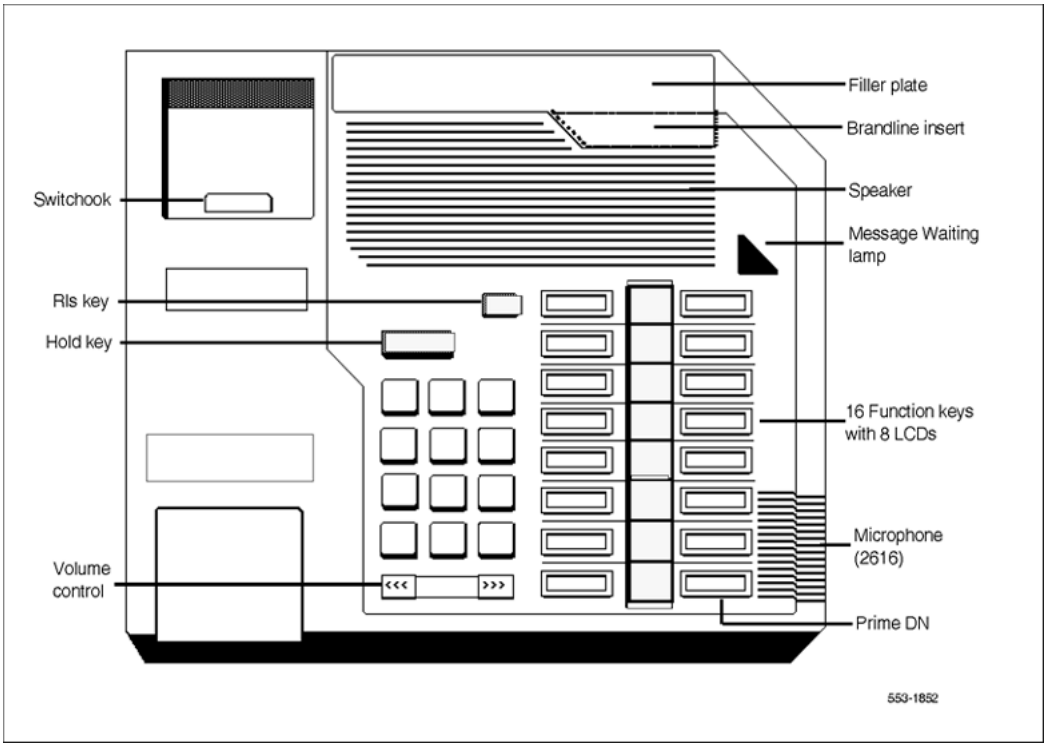


Figure 3: M2216, M2016S and M2616 set

Table 5: M2216 Telephone test

Step	Key operated	LCD location and response	Display and Tones
Note: Do not test key 7			
	Feature keys:		
1	Key 0	LCD 0 lit	display upper case letters
2	Key 1	LCD 1 lit	display lower case letters
3	Key 2	LCD 2 lit	display clear
4	Key 3	LCD 3 lit	display darkens
5	Key 4	LCD 4 lit	top line of display darkens
6	Key 5	LCD 5 lit	turn Message Waiting LED on
7	Key 6	LCD 6 lit	turn Message Waiting LED off
8	Key n>7	LCD n lit	
	Keypad keys:		
9	Key 1	LCD 0 lit	1 on display

Step	Key operated	LCD location and response	Display and Tones
10	Key 2	LCD 1 lit	2 on display
11	Key 3	LCD 2 lit	3 on display
12	Key 4	LCD 3 lit	4 on display
13	Key 5	LCD 4 lit	5 on display
14	Key 6	LCD 5 lit	6 on display
15	Key 7	LCD 6 lit	7 on display
16	Key 8	LCD 0 and 6 lit	78 on display
17	Key 9	LCD 1 and 6 lit	9 on display
18	Key 0	LCD 2 and 6 lit	0 on display
19	Key *	all LCDs lit	bottom line of display darkens
20	Key #	all LCDs off	display clear
	Fixed keys:		
21	HLD	LCD 0 to 4 lit	dial tone
22	HLD	LCD 0 to 4 lit	buzzer
23	HLD	end of test	

Table 6: M2016S and M2616 Telephone test

Step	Key operated	LCD location and response	Display and Tones
Note: Do not test key 7			
	Feature keys:		
1	Key 0	LCD 0 lit	display upper case letters
2	Key 1	LCD 1 lit	display lower case letters
3	Key 2	LCD 2 lit	display clear
4	Key 3	LCD 3 lit	display darkens
5	Key 4	LCD 4 lit	top line of display darkens
6	Key 5	LCD 5 lit	turn Message Waiting LED on
7	Key 6	LCD 6 lit	turn Message Waiting LED off
8	Key n>7	LCD n lit	
	Keypad keys:		

Step	Key operated	LCD location and response	Display and Tones
9	Key 1	LCD 0 lit	1 on display
10	Key 2	LCD 1 lit	2 on display
11	Key 3	LCD 2 lit	3 on display
12	Key 4	LCD 3 lit	4 on display
13	Key 5	LCD 4 lit	5 on display
14	Key 6	LCD 5 lit	6 on display
15	Key 7	LCD 6 lit	7 on display
16	Key 8	LCD 0 and 6 lit	8 on display
17	Key 9	LCD 1 and 6 lit	9 on display
18	Key 0	LCD 2 and 6 lit	0 on display
19	Key *	all LCDs lit	top line of display darkens
20	Key #	all LCDs off	display clear
	Fixed keys:		
21	Handsfree	LCD 15 lit	
22	Release	all LCDs off	
23	HLD	LCD 0 to 4 lit	dial tone from speaker
24	Off-hook	all LCDs flash	dial tone from handset
25	On-hook	all LCDs fast flash	dial tone from speaker
26	Off-hook	all LCDs lit	display darkens
27	On-hook	all LCDs off	display clear
28	HLD	LCD 0 to 4 lit	buzzer
29	HLD	end of test	

M2317 Telephone test

The key and LCD layout is shown in Figure 4: M2317 Series Telephone Key and LCD Layout on page 72. The test is provided in Table 7: M2317 Telephone test on page 72.

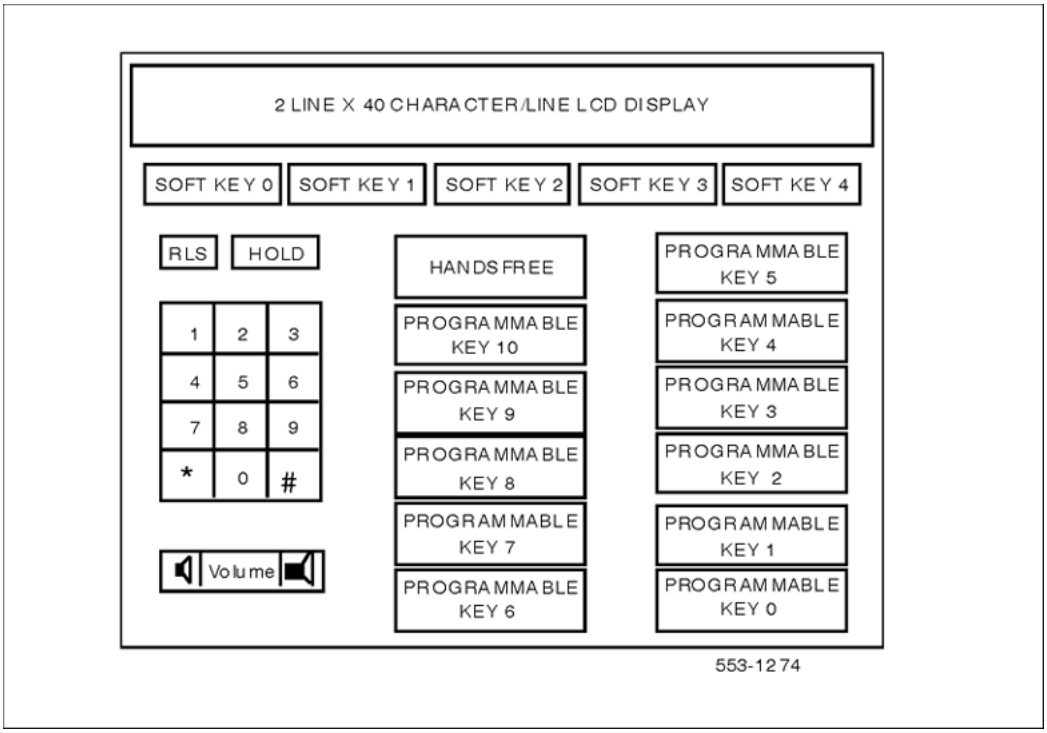


Figure 4: M2317 Series Telephone Key and LCD Layout

Table 7: M2317 Telephone test

Step	Key operated	LCD location & response	Display and Tones
1	Press *	All LCD are lit	Blank
2	Off-hook	All LCDs flash (except Key 11)	192
3	On-hook	All LCDs fast flash (except Key 11)	192
4	Off-hook	All LCDs lit	All 80 character elements (40 characters x 2 lines) are fully lit. Each character element is made up of 35 dots in a 5 x 7 dot array.
5	On-hook	All LCDs off	All 80 character elements are off
	Dial Pad Keys:		
6	Key 1	LCD 0 lit	1
7	Key 2	LCD 1 lit	12
8	Key 3	LCD 2 lit	123

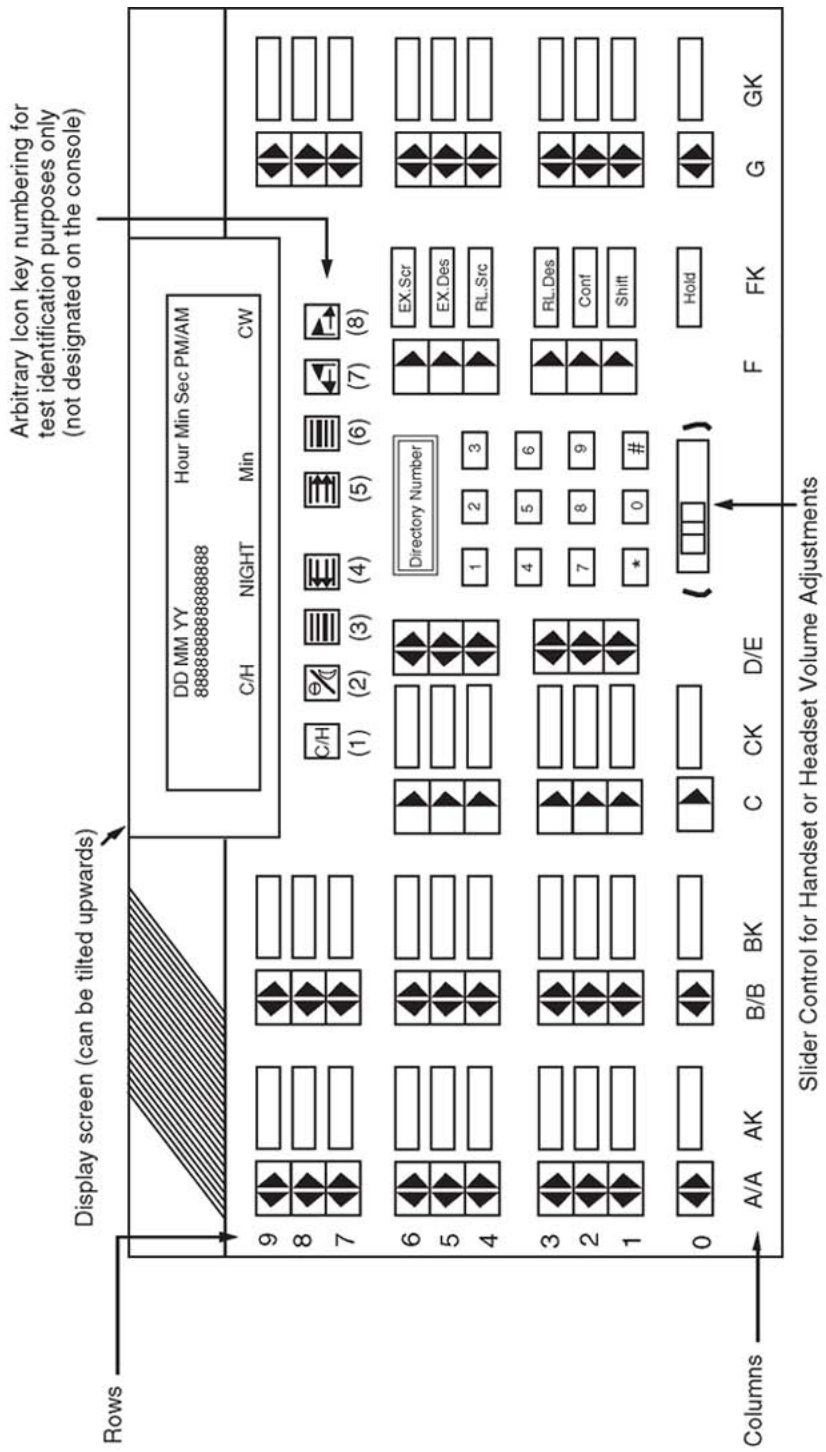
Step	Key operated	LCD location & response	Display and Tones
9	Key 4	LCD 3 lit	1234
10	Key 5	LCD 4 lit	12345
11	Key 6	LCD 5 lit	123456
12	Key 7	LCD 6 lit	1234567
13	Key 8	LCD 7 lit	12345678
14	Key 9	LCDs 0 & 7 lit	123456789
15	Key 0	LCDs 1 & 7 lit	1234567890
16	Key 1	LCD 0 lit	12345678901
17	Key 2	LCD 1 lit	123456789012
18	Key 3	LCD 2 lit	1234567890123
19	Key 4	LCD 3 lit	12345678901234
20	Key 5	LCD 4 lit	123456789012345
21	Key 6	LCD 5 lit	1234567890123456
22	Key 7	LCD 6 lit	12345678901234567
23	Key 8	LCD 7 lit	123456789012345678
24	Key 9	LCDs 0 & 7 lit	1234567890123456789
25	Key 0	LCDs 1 & 7 lit	12345678901234567890
26	Key 1	LCD 0 lit	12345678901234567890 1
27	Key 2	LCD 1 lit	12345678901234567890 12
28	Key 3	LCD 2 lit	12345678901234567890 123
29	Key 4	LCD 3 lit	12345678901234567890 1234
30	Key 5	LCD 4 lit	12345678901234567890 12345
31	Key 6	LCD 5 lit	12345678901234567890 123456
32	Key 7	LCD 6 lit	12345678901234567890 1234567
33	Key 8	LCD 7 lit	12345678901234567890 12345678
34	Key 9	LCDs 0 & 7 lit	12345678901234567890 123456789
35	Key 0	LCDs 1 & 7 lit	12345678901234567890 1234567890

Step	Key operated	LCD location & response	Display and Tones
36	Key 1	LCD 0 lit	12345678901234567890 12345678901234567890 1
37	Key 2	LCD 1 lit	12345678901234567890 12345678901234567890 12
38	Key 3	LCD 2 lit	12345678901234567890 12345678901234567890 123
39	Key 4	LCD 3 lit	12345678901234567890 12345678901234567890 1234
40	Key 5	LCD 4 lit	12345678901234567890 12345678901234567890 12345
41	Key 6	LCD 5 lit	12345678901234567890 12345678901234567890 123456
42	Key 7	LCD 6 lit	12345678901234567890 12345678901234567890 1234567
43	Key 8	LCD 7 lit	12345678901234567890 12345678901234567890 12345678
44	Key 9	LCDs 0 & 7 lit	12345678901234567890 12345678901234567890 123456789
45	Key 0	LCDs 1 & 7 lit	12345678901234567890 12345678901234567890 1234567890
46	Key *	All LCD lit (except Key 11)	88888888888888888888 88888888888888888888
47	Key #	All LCD go off	Display clears
	Programmable Keys:		
48	Key 0	LCD 0 lit	Blank
49	Key 1	LCD 1 lit	Blank
50	Key 2	LCD 2 lit	Blank
51	Key 3	LCD 3 lit	Blank
52	Key 4	LCD 4 lit	Blank
53	Key 5	LCD 5 lit	Blank
54	Key 6	LCD 6 lit	Blank

Step	Key operated	LCD location & response	Display and Tones
55	Key 7	LCD 7 lit	Blank
56	Key 8	LCD 8 lit	Blank
57	Key 9	LCD 9 lit	Blank
58	Key 10	LCD 10 lit	Blank
	Soft Keys:		
59	Key 0	LCD 0 flashes 60 ipm	ABCDEFGHIJKLMNOPQRST UVWXYZABCDEFGH
60	Key 1	LCD 1 flashes 60 ipm	Display clears
61	Key 2	LCD 2 flashes 60 ipm	abcdefghijklmnopqrst uvwxyzabcdefghijklmn
62	Key 3	LCD 3 flashes 60 ipm	Display clears
63	Key 4	LCD 4 flashes 60 ipm	Display clears
64	Press HOLD key	LCD 0 to 4 light steadily (Key 11 lit)	Dial tone heard through speaker
65	Handset off-hook	All LCD flash at 60 ipm (Key 11 off)	Dial tone heard through handset
66	Handset on-hook	All LCD fast flash at 120 ipm (Key 11 on)	Dial tone heard through speaker
67	Press HANDSFREE key	LCD 0 to 2 light steadily	
68	Press RELEASE key	All LCD go off	
69	Press HOLD key	LCD 0 to 4 light steadily	Buzz heard through speaker
70	Press HOLD key	End of test	

M2250 Console test

The M2250 faceplate is shown in Figure 5: M2250 Console - Key and LCD Layout on page 76. The tests are provided in the Table 8: M2250 Console test on page 77.



Note: This illustration is not drawn to scale. Some of the designations shown are not marked on the console but are given here for identification purposes only when running the Attendant Console Indicator and Tone Tests in accordance with Tables 2-A and 2-B.

Figure 5: M2250 Console - Key and LCD Layout

M2250 Console test

Table 8: M2250 Console test

Step	Key operated	LCD location and response	Display and Tones
1	Select idle loop key		
2	Enter SPRE code 92	All LCDs lit except F1	888888888888888888. . . 888888888888888888. . .
3	Press dial pad #	All off	Active
4	Press dial key 1	D1 lit	1
5	Press dial key 2	E1 lit	12
6	Press dial key 3	D2 lit	123
7	Press dial key 4	E2 lit	1234
8	Press dial key 5	D3 lit	12345
9	Press dial key 6	E3 lit	123456
10	Press dial key 7	D4 lit	1234567
11	Press dial key 8	E4 lit	12345678
12	Press dial key 9	D5 lit	123456789
13	Press dial key 0	E5 lit	1234567890
14	Repeat step 4 untilb oth lines of the display are full		12345678901234567. . . 12345678901234567. . .
15	Press dial pad *	All LCDs lit except F1	888888888888888888. . . 888888888888888888. . .
16	Press dial pad #	All LCD blank	ACTIVE
17	Press AK key 0	AR0 lit	ABCDEFGHIJKLMNOP. . . NOPQRSTUVWXYZAB. . .
18	Press AK key 1	AR1 lit	abcdefghijklmnopqrstuvwn opqrstuvwxyzabcdefg
19	Press AK key 2	AR2 lit	Display shows series of dark squares
20	Press AK key 3	AR3 lit	ACTIVE
21	Press AK key 4	AR4 lit	ACTIVE

Step	Key operated	LCD location and response	Display and Tones
22	Press AK key 5	AR5 lit	ACTIVE
23	Press AK key 6	AR6 lit	ACTIVE
24	Press AK key 7	AR7 lit	ACTIVE
25	Press AK key 8	AR8 lit	ACTIVE
26	Press AK key 9	AR9 lit	ACTIVE
27	Press BK key 0	BR0 lit	ACTIVE
28	Press BK key 1	BR1 lit	ACTIVE
29	Press BK key 2	BR2 lit	ACTIVE
30	Press BK key 3	BR3 lit	ACTIVE
31	Press BK key 4	BR4 lit	ACTIVE
32	Press BK key 5	BR5 lit	ACTIVE
33	Press BK key 6	BR6 lit	ACTIVE
34	Press BK key 7	BR7 lit	ACTIVE
35	Press BK key 8	BR8 lit	ACTIVE
36	Press BK key 9	BR9 lit	ACTIVE
37	Press CK key 0	C0 lit	IDLE
38	Press CK key 1	C1 lit	ACTIVE
39	Press CK key 2	C2 lit	ACTIVE
40	Press CK key 3	C3 lit	ACTIVE
41	Press CK key 4	C4 lit	ACTIVE
42	Press CK key 5	C5 lit	ACTIVE
43	Press CK key 6	C6 lit	ACTIVE
44	Press Icon key 1		C/H and ACTIVE
45	Press Icon key 2		BUSY
46	Press CK key 0	C0 lit	IDLE
47	Press GK key 0	GRO lit	ACTIVE
48	Press GK key 1	GR1 lit	ACTIVE
49	Press GK key 2	GR2 lit	ACTIVE
50	Press GK key 3	GR3 lit	ACTIVE
51	Press GK key 4	GR4 lit	ACTIVE
52	Press GK key 5	GR5 lit	ACTIVE

Step	Key operated	LCD location and response	Display and Tones
53	Press GK key 6	GR6 lit	ACTIVE
54	Press GK key 7	GR7 lit	ACTIVE
55	Press GK key 8	GR8 lit	ACTIVE
56	Press GK key 9	GR9 lit	ACTIVE
57	Press FK key 1	G9 and F1 lit	[S] ACTIVE
58	Press AK key 0	AL0 and F1 lit	[S] ACTIVE
59	Press AK key 1	AL1 and F1 lit	[S] ACTIVE
60	Press AK key 2	AL2 and F1 lit	[S] ACTIVE
61	Press AK key 3	AL3 and F1 lit	[S] ACTIVE
62	Press AK key 4	AL4 and F1 lit	[S] ACTIVE
63	Press AK key 5	AL5 and F1 lit	[S] ACTIVE
64	Press AK key 6	AL6 and F1 lit	[S] ACTIVE
65	Press AK key 7	AL7 and F1 lit	[S] ACTIVE
66	Press AK key 8	AL8 and F1 lit	[S] ACTIVE
67	Press AK key 9	AL9 and F1 lit	[S] ACTIVE
68	Press GK key 0	GL0 and F1 lit	[S] ACTIVE
69	Press GK key 1	GL1 and F1 lit	[S] ACTIVE
70	Press GK key 2	GL2 and F1 lit	[S] ACTIVE
71	Press GK key 3	GL3 and F1 lit	[S] ACTIVE
72	Press GK key 4	GL4 and F1 lit	[S] ACTIVE
73	Press GK key 5	GL5 and F1 lit	[S] ACTIVE
74	Press GK key 6	GL6 and F1 lit	[S] ACTIVE
75	Press GK key 7	GL7 and F1 lit	[S] ACTIVE
76	Press GK key 8	GL8 and F1 lit	[S] ACTIVE
77	Press GK key 9	GL9 and F1 lit	[S] ACTIVE
78	Press Hold key	F1 and B0-4 lit	[S] Busy tone in handset
79	Press Hold key	F1 and B0-4 lit	[S] Buzz in speaker
80	Press Hold key	F1 and C0 lit	[S] NIGHT or BUSY
81	Press CK key 1	F1 and C1 lit	[S] NIGHT or BUSY
82	Dial SPRE 92	All LCDs lit	888888888888888888. . . 888888888888888888. . .

Step	Key operated	LCD location and response	Display and Tones
83	Press dialpad #	F1 lit	[S] ACTIVE
84	Press FK key 1		ACTIVE
85	Press FK key 2	All LCDs lit except F1	888888888888888888. . . 888888888888888888. . .
86	Press FK key 2	LCDs Flash at 120 ipm	Flash ACTIVE/NIGHT
87	Press FK key 2	LCDs Flash at 60 ipm	888888888888888888. . . 888888888888888888. . .
88	Press FK key 2	LCDs Flash at 30 ipm	Flash ACTIVE/NIGHT
89	Press Icon key 8	All LCDs off	ACTIVE
90	Press Icon key 7	B0-4 lit	ACTIVE, dial tone
91	Press FK key 5	All LCDs off	ACTIVE, dial tone
92	Press Icon key 7	B0-4 lit	ACTIVE
93	Press FK key 5	All LCDs off	ACTIVE
94	Press FK key 6	B0-4 lit	ACTIVE
95	Press FK key 6	All LCDs off	ACTIVE
96	Handset out	All LCDs off	ACTIVE
97	Handset in	B0-4 lit	ACTIVE
98	Handset out	All LCDs off	ACTIVE
99	Handset in other side of console	B0-4 lit	ACTIVE
100	Press Hold key	B0-4 lit	ACTIVE, busy tone
101	Press Hold key	B0-4 lit	ACTIVE, Buzz in speaker
102	Press Hold key	C0 lit	NIGHT
103	End of test		

Chapter 10: LD 32: Network and Peripheral Equipment Diagnostic

LD 32 performs checks and maintenance functions on network and Peripheral Signaling equipment. LD 32 will allow commands to be used for XTD cards. The STAT command will produce an output which has XTD, LDC or LGD appended where required.

On Small Systems, Avaya Communication Server 1000S, MG 1000B, and MG 1000T, this program can be used to:

- get the status of peripheral equipment cards and units
- enable and disable peripheral equipment cards and units
- initiate or cancel flash downloads for M39xx units
- query and print the firmware versions currently on M39xx units
- reset or clear directory password for M39xx units
- test message waiting lamps on 500/2500 telephone sets
- print set and card IDs
- convert packed TNs in hex to the card and unit format

On Large Systems and CS 1000E Systems, this program is used to:

- get the status of Peripheral Signaling (PS), Controller and network cards
- get the status of IPE shelves cards and units
- disable and enable PS, Controller and network cards
- disable and enable IPE shelves, cards and units
- initiate or cancel flash downloads for M39xx units
- query and print the firmware versions currently on M39xx units
- reset or clear directory password for M39xx units
- test message waiting lamps on 500/2500 sets
- test Message Waiting Lamps (MWL) on 2500 sets during midnight routines
- print set and card IDs on superloops
- convert packed TNs in hex to the loop, shelf, card, unit format

Note:
Disabled DID trunks are placed in the answer state while disabled.

Note:
If Recorded Telephone Dictation (RTDT) cards are to be software enabled or disabled, the Out-of-Service (OS) lead should be connected to ground. On completion of the task, ground can be removed.

Note:
Card ID information is presented as follows:

```
CCCCCCCC-RRSSSS
```

Where:

`CCCCCCCC` = is the order code `RR` = is the release number `SSSS` = is the serial number

Note:
After making any changes to the route data block, IPE TRUNK CARDS MUST BE DOWNLOADED by issuing the ENLC l s c command.

Note:
When getting the status of a card relating to a trunk error (STAT), the term RVSD may appear with the trunk information. RVSD indicates that the software detected a reversed wired trunk for that unit.

Overlay 32 linkage

Overlay programs 10, 11, 20 and 32 are linked, thus eliminating the need to exit one Overlay and enter another. Once one of the aforementioned Overlays has been loaded, it is possible to add, print and obtain the status of a set without having to exit one Overlay and load another.

Input processing has also been enhanced. Prompts ending with a colon (:) allow the user to enter either:

1. a question mark (?) followed by a carriage return (<CR>) This entry will present you with a list of valid responses to that prompt.
2. an abbreviated response The system responds to this entry with the nearest match. If there is more than one possible match, the system responds with SCH0099, the input followed by a question mark, and a list of possible responses. The user can then enter a valid response.

Using Enable/Disable commands

All units on a loop go into maintenance busy mode when disabled using the DISL command. The shelves on a loop must be individually re-enabled via the ENLS command. Any telephones that were in lockout mode show as idle, then go into lockout mode again 30 seconds after any unit on the shelf requests dial tone.

On Small Systems, CS 1000S, MG 1000B, and MG 1000T the DISL and ENLL commands are not available. Instead, use the DISS, ENLC, DISC and ENLS commands as described below.

When enabling a network loop serving ISDLC cards, the ISDLC cards must be individually disabled then re-enabled to ensure that service is restored to digital telephones. Service may also be restored to digital telephones by disconnecting, and then reconnecting the telephone's line cord.

Note:
When the Trunk Failure Monitor (TFM) package is enabled, a failed trunk is displayed as BUSY. The enable/disable command does not enable or disable the failed trunk unit (it stays in the BUSY state.)

Note:
When the French Type Approval package (FRTA 197) is enabled then CO trunk units are not busied when they are disabled.

Fibre Network Fabric

The Fibre Network Fabric extends and enhances the 5-group network architecture to 8 non-blocking (inter-group) Network groups, with a resulting expansion in network capacity to 8k timeslots available for Intergroup traffic.

This is achieved by using OC-12 SONET rings, and adding additional network and IPE shelves, cards and cables and software changes to allow using the expanded network capacity. This expansion increases the number of available loops from 160 to 256. This applies to Multi Group systems only.

Basic commands

Contents

Section
The following commands are applicable to all systems.
Large System and Avaya Communicatuon Server 1000E System commands on page 85
Small Systems, CS 1000S, MG 1000B, and MG 1000T commands
Superloop commands on page 87
ISDN BRI MISP commands on page 88
Small Systems, CS 1000S, MG 1000B, and MG 1000T BRI MISP commands
ISDN BRI SILC/UILC commands on page 89
Small Systems, CS 1000S, MG 1000B, and MG 1000T BRI SILC/UILC commands
ISDN BRI BRSC commands on page 90
System commands on page 91

Basic commands

The following commands are applicable to all systems.

CMIN	Clears minor alarm for all customers
CMIN ALL	Clears minor alarm for all customers
CONV tn	Convert packed TN (in hex) to loop, shelf, card and unit format
DIS VTRM <cust> <rout>	Disables all IP Peer Virtual Trunk TNs in the specified route associated with the specified customer and the associated DCIP.
END	Abort current test

ENL VTRM <cust> <rout>	
	Enables all IP Peer Virtual Trunk TNs in the specified route associated with the specified customer and the associated DCIP.
FDLC	Cancel or stop the sytem wide flash download for M39xx units
FDLS	Initiate system wide flash download according to the FDL schedule programmed in Overlay 97
FSUM	Print summary report of firmware versions currently on M39xx units
FSUM ALL	Print complete report of all M39xx sets based on parameters specified in LD 97.
STAT VTRM <cust> <route> <starting member> <number of members>	
	Displays the status of the virtual trunks for a customer's route starting from a specified starting member for the number of members specified.

Large System and Avaya Communicatuon Server 1000E System commands

CDSP	Clear the maintenance display on active CPU to 00 or blank
CMIN	Clears minor alarm for all customers
CMIN ALL	Clears minor alarm for all customers
CONV tn	Convert packed TN (in hex) to loop, shelf, card and unit format
CONV l s c u	Convert loop, shelf, card and unit format to packed TN (in hex)
CPWD l s c u	Reset or Clear directory password for M3903, M3904 and M3905 telephone
DISC l s c	Disable specified peripheral card
DISI l s c	Disable specified card when it is idle
DISL l	Disable network loop
DISS l s	Disable specified shelf
DISU l s c u	Disable specified unit
DSCT l	Disable automatic background continuity tests for superloop
DSNW l	Disable network card containing specified loop

DSPS x	Disable Peripheral Signaling card x
DSXP x	Disable controller x and all connected cards
END	Abort current test
ENLC l s c	Enable and reset specified peripheral card
ENLG x	Enable group x
ENLL l	Enable network loop
ENLR l s c u	Enable specified DTR/MFR card or unit. **Note:** This is a small systems specific command.
ENLS l s	Enable specified shelf
ENLU l s c u	Enable specified unit
ENNW l	Enable network card with specified loop
ENPS x	Enable PS card x and associated loops
FDLC	Cancel or stop the sytem wide flash download for M39xx units
FDLF l s c u	Initiate forced download to one M39xx unit regardless of version or state
FDLI l s c u	Initiate download to one M39xx unit when the set becomes idle, if the set's firmware is not current.
FDLU l s c u	Initiate download to one M39xx unit, if the set's firmware is not current.
FDLS	Initiate system wide flash download according to the FDL schedule programmed in Overlay 97
FSUM	Print summary report of firmware versions currently on M39xx units
FSUM ALL	Print complete report of all M39xx sets based on parameters specified in LD 97.
FWVU l s c u	Query and print the firmware versions currently on M39xx terminal
LBD l s	List TN of all PBX units on specified shelf, with lamps flagged as defective.
LBSY l s	List TNs of all busy units on specified shelf
LDIS l s	List TNs of all disabled units on specified shelf
LIDL l s	List TNs of all idle units on specified shelf
LLBD l s	List TNs of 500/2500 sets with defective MWLs

LMNT l s	List TNs of all maintenance busy units on specified shelf
PBXH	Message Waiting lamp maintenance
PBXT ALL	Test all Message Waiting lamps
PBXT l (s c u)	Test Message Waiting lamps on loop (or shelf or card or unit)
STAT	Get status of all configured loops in system
STAT l	Give status of one or all loops
STAT l s	Get idle, busy or disabled status of units on specified shelf
STAT l s c	Get status of specified card
STAT l s c u	Get status of specified unit
STAT NWK l	Check status of network card with specified loop
STAT PER x	Get status of PS card x
TRK l s c u	Seize specified trunk for outpulsing

Superloop commands

Note:
The Loop level commands are not supported for Small Systems, CS 1000S, MG 1000B, and MG 1000T systems.

DISL sl	Disable specified superloop
DSCT sl	Disable automatic background continuity tests for a superloop
DSXP x	Disable Controller x and all associated IPE cards
ENCT sl	Enable automatic background continuity tests for a superloop
ENLL sl (v)	Enable superloop, download peripheral software version v
ENLL sl	Enable specified Superloop
ENXP x (v)	Enable Controller x and associated IPE cards, download software version v
ENXP XPC x (v)	Enable Controller x, do not enable the associated IPE cards, download software version v
IDC sl	Print Card ID for superloop and associated Controller(s)
IDC l s c	Print card ID for IPE card

IDC sl	Get card id of LCI sl and its associated RCI
IDCS x	Print card ID for all cards on shelf controlled by Controller x
IDU l s c u	Print set ID
IDU <TN>	Prints the MAC address, Model Vendor, software version, Set IP address.
LBSY l s	List TNs of all busy units on specified shelf
LDIS l s	List TNs of all disabled units on specified shelf
LIDL l s	List TNs of all idle units on specified shelf
STAT sl	Get status of superloop and separate carriers on that superloop
SUPL (sl)	Print data for one or all superloops
XNTT sl	Do self-test of Network card for specified superloop
XPCT x	Do self-test on Controller x
XPEC (x)	Print data for one or all Controllers

Note:
If a trunk unit is controlled by APNSS, the STAT commands will indicate this is an APNSS trunk and will also display the status of the D-channel. The display format remains the same.

ISDN BRI MISP commands

The following commands are available for ISDN Basic Rate Interface Multi-purpose ISDN Signaling Processor (MISP) cards.

DISL l	Disable MISP loop
DISL (appl) l	Disable specified application on MISP loop
DISL (appl) l 1	Disable and remove specified application from MISP loop
DISL (appl) l REM	Disable and remove specified application from MISP loop
DLIF l x	Download an UIPE BRI trunk interface data file to an MISP loop
ENLL l	Enable MISP loop
ENLL l FDL	Enable specified MISP loop and force download (FDL) basecode

ENLL (appl) l	Enable specified application on MISP loop
ENLL (appl) l 1	Enable specified application on MISP loop and force download the application loadware onto the MISP
ENLL (appl) l FDL	Enable specified application on MISP loop and force download the application loadware onto the MISP
IDC l	Print MISP card ID
PERR (appl) l	Upload error log for specified MISP
STAT l s	Get idle, busy or disabled status of units on specified shelf
STAT (appl) l	Get status of MISP loop (and application)

ISDN BRI SILC/UILC commands

The following commands are available for ISDN Basic Rate Interface S/T-Interface line (SILC) or U-Interface line (UILC) cards and the associated Digital Subscriber Loops (DSL).

DIS AUTO l s c u	Disable automatic link recovery option of a DSL
DISC l s c	Disable S/T-Interface line (SILC) or U-Interface line (UILC) card
DISI l s c	Disable specified card when it is idle
DISU l s c d	Disable specified Digital Subscriber Loop (DSL) (0-7)
DSRB l s c d	Disable Remote Loop Back for specified BRI Trunk DSL
DSTS l s c d	Disable Remote Loop Back test mode for specified BRI Trunk DSL
ENL AUTO l s c u	Enable automatic link recovery option of a DSL
ENLC l s c	Enable S/T-Interface line (SILC) or U-Interface line (UILC) card
ENLU l s c d	Enable specified unit Digital Subscriber Loop (DSL) (0-7)
ENRB l s c d	Enable Remote Loop Back for specified BRI Trunk DSL
ENTS l s c d	Enable Remote Loop Back test mode for the specified BRI Trunk DSL
ESTU l s c d	Establish D-channel link for specified DSL
FDIS NCAL <l s c DSL#> <conn_ID>	Force disconnect the specified call-independent connection

IDC l s c	Print SILC/UILC card ID
PCON l s c d	Print configuration and LAPD parameters for specified BRI Trunk DSL
PERR (appl) l s c	Print protocol log for specified BRI line card
PLOG l s c d	Print protocol log for specified BRI Trunk DSL
PMES l s c d	Print Layer 3 message log for specified BRI Trunk DSL
PTAB l s c d	Upload and print Layer 3 Message configuration IE table for specified BRI Trunk DSL
PTAB l s c d <tbl #>	Upload and print specified Layer 3 Message configuration IE table for specified BRI Trunk DSL
PTRF l s c d	Print traffic data for specified BRI Trunk DSL
RLBT l s c d	Perform Remote Loop Back test on specified BRI Trunk DSL
RLSU l s c d	Release D-channel link for specified DSL
STAT l s c	Get status of specified SILC or UILC
STAT l s c d	Get status of specified Digital Subscriber Loop 0-7
STAT NCAL <l s c DSL#>	List all current call-independent connections on a given BRI DSL. **Note:** This is applicable for UIPE protocol-based DSLs only, for which the CS 1000 supports call-independent connections ("GF capability").
STAT NCAL <l s c DSL#> <conn_ID>	List information pertaining to a specific call-independent connection

ISDN BRI BRSC commands

The following commands are available for the ISDN Basic Rate Signaling Concentrator (BRSC) card.

DISC BRI l s c	Disable the BRSC ISDN BRI application.
DISC (BASE) l s c	Disable specified card.

ENLC (BASE) l s c (FDL/NST)	Enable specified card.
ENLC BRI l s c (FDL)	Enable the BRSC ISDN BRI application.
IDC l s c	Print BRSC card and loadware version.
STAT l s c	Get status of specified card.

System commands

The following commands are available:

DSRM <cust #> <route #>	Disables all route members in a customer's route. It will disconnect all active calls associated with the trunks, disable all route members on the call server, unregister all trunks and remove them from the RLM table. On the Signaling Server side, all trunks will be removed from the Signaling Server list.
ECNT CARD l s c <customer>	Prints the number of IP Phones registered for the specified card. If <customer> is specified, the count is specific to that customer (note that a card must be specified to enter a customer.) Otherwise, the count is across all customers. If no parameters are entered, the count is printed for all zones. A partial TN can be entered for the card (L or L S) which then prints the count per that parameter (a customer cannot be specified in this case).
ECNT NODE nodeNum	Prints the number of IP Phones registered for the specified node. If no parameter is entered, the count is printed for all nodes.
ECNT SS <hostName>	Prints the number of IP Phones registered for the specified signaling server. If no parameter is entered, the count is printed for all signaling servers. **Note:** If the hostName variable contains an underscore (_), then an NPR001 error message is returned, as an underscore is considered to be an invalid character.
ECNT ZONE zoneNum <customer>	

	Prints the number of IP Phones registered for the specified zone. If <customer> is specified, the count is specific to that customer (note that a zone must be specified to enter a customer). Otherwise, the count is across all customers. If no parameters are entered, the count is printed for all zones. If the IP Phone is in VO login state, and Current Zone (CUR_ZONE) is different from the Configured Zone (CFG_ZONE), both zones are counted for the ECNT command.
ENRM <cust #> <route #>	Enable all the virtual trunk route members in a customer's route. It will enable all route members, register them and put them into the RLM table. On the Signaling Server side, all trunks will be put on the Signaling Server list.

STVT <cust #> <route #> <starting member> <number of members>

Displays the status of the virtual trunks for a customer's route starting from a specified starting member for the number of members specified.

STAT VTRM <cust #> <route #> <start member> <end member>

Display the status of the virtual trunks specified by customer, route, start member and end member numbers.

Alphabetical list of commands

Command	Description	Pack/Rel
CDSP	Clear the maintenance display on active CPU to 00 or blank.	basic-1
CMIN	Clears minor alarm for all customers	alrm_filter-22
CMIN ALL	Clears minor alarm for all customers	basic-1
CONV tn	Convert packed TN (in hex) to l s c u, or vice versa.	xpe-15
c u	Small Systems, CS 1000S, MG 1000B, and MG 1000T	
CONV tn	Convert packed TN (in hex) to l s c u	xpe-15
l s c u	Convert packed TN (in hex) to tn	

Command	Description	Pack/Rel
	The command format is: • CONV tn - convert packed TN • CONV l s c u - convert unpacked TN	
	Where: l = 0-255, System with Fibre Network Fabric	fnf-25
CPWD l s c u c u	Reset or Clear directory password Small Systems, CS 1000S, MG 1000B, and MG 1000T	basic-24
	Allows the Directory password of the specified set to be reset to default (12345678). This allows a user to access the Directory if the password has been forgotten or if the user wants to change the current password. Applies to M3903, M3904, M3905, and IP Phone 2004.	itg-25
	For M3900 Phase 3 terminals the Directory password is cleared.	
	Where: l = 0-255, System with Fibre Network Fabric	fnf-25
DIS AUTO l s c u c u	Disable automatic link recovery option of a DSL Small Systems, CS 1000S, MG 1000B, and MG 1000T format	bri-18
DISC (appl) c	Disable application on Multi-purpose ISDN Signaling Processor (MISP) (Small Systems, CS 1000S, MG 1000B, and MG 1000T). Where: appl =BRIL (Basic Rate Interface Line), BRIT (Basic Rate Interface Trunk), or BRIE (UIPE Basic Rate Interface Trunk)	bri-18
DISC (appl) c REM		bri-18
	Disable and remove application from Multi-purpose ISDN Signaling Processor (MISP) (Small Systems, CS 1000S, MG 1000B, and MG 1000T). Where: appl =BRIL (Basic Rate Interface Line), BRIT (Basic Rate Interface Trunk), or BRIE (UIPE Basic Rate Interface Trunk)	
DISC (BASE) lsc	Disable specified BRSC card or to disable the ISDN Basic Rate Interface Signaling Concentrator (BRSC) card, where: • BASE = Disable only the basecode. If not specified, both the basecode and application are disabled. The application is disabled first unless BASE is entered. • l = loop	bri-18

Command	Description	Pack/Rel
	• s = shelf • c = card The card faceplate LED is turned on to indicate the card is disabled, and the IPC channel is eliminated. The "." prompt is given when the process is complete.	
DISC BRI l s c	Disable the BRSC ISDN BRI application. All active and transient ISDN BRI calls are dropped, and all signaling and packet channels are torn down. The DSL software state remains the same, but the ISDN BRI line cards receive a disable message.	bri-18
DISC c	Disable specified DTR/MFR card. (Small Systems, CS 1000S, MG 1000B, and MG 1000T) This command is also used for Multi-purpose ISDN Signaling Processor (MISP). If BRI reference clock source is configured on this SILC the user will be prompted with: `CLOCK SOURCE ON DSL #, PROCEED? ,` Where # = unit 0-7 For Small Systems, CS 1000S, MG 1000B, and MG 1000T: DISC 0 disables all configured units on card 0	basic-1
DISC l s c	Disable specified peripheral card. If BRI reference clock source is configured on this SILC the user will be prompted with: `CLOCK SOURCE ON DSL #, PROCEED? ,` Where # = unit 0-7 **Note:** For MGX, cards 8,9 and 10 are treated as one card. Issuing a command for card 8 also affects cards 9 and 10. Issuing a command for card 9 also affects card 10. Issuing a command for card 10 only affects card 10.	basic-1
DISI c	Disable specified card when it is idle. (Small Systems, CS 1000S, MG 1000B, and MG 1000T) If BRI reference clock source is configured on this SILC the user will be prompted with: `CLOCK SOURCE ON DSL #, PROCEED? ,` Where # = unit 0-7	basic-1
DISI l s c	Disable specified card when it is idle.	basic-1

Command	Description	Pack/Rel
	Where: l = 0-255, System with Fibre Network Fabric If BRI reference clock source is configured on this SILC the user will be prompted with: `CLOCK SOURCE ON DSL #, PROCEED? ,` Where # = unit 0-7 **Note:** For MGX, cards 8,9 and 10 are treated as one card. Issuing a command for card 8 also affects cards 9 and 10. Issuing a command for card 9 also affects card 10. Issuing a command for card 10 only affects card 10.	fnf-25
DISL (appl) l	Disable application on MISP loop. Where appl = • BRIL (Basic Rate Interface Line), or • BRIT (Basic Rate Interface Trunk)	bri-18
DISL (appl) l 1	Disable MISP loop. Where: appl =BRIL (Basic Rate Interface Line), BRIT (Basic Rate Interface Trunk), or BRIE (UIPE Basic Rate Interface Trunk). Applicable if SUPP package 131 is not equipped.	bri-18
DISL (appl) l 1	Disable MISP application and loop. Where: • appl = optional application name (BRIL) • 1 = force download the application	bri-18
DISL (appl) l REM	Disable and remove application from Multi-purpose ISDN Signaling Processor (MISP.) Applicable if SUPP package 131 is equipped.	bri-18
DISL l	Disable network loop. See "Using the Enable/Disable commands" in the introduction. This command is also used for superloops and MISPs.	basic-1
DISL sl	Disable specified superloop. Active calls on the superloop will be disconnected and line transfer will occur at the remote end.	basic-21
DISS l s	Disables specified shelf. See "Using the Enable/Disable commands" in the introduction.	basic-1

Command	Description	Pack/Rel
DISS m	Disables specified module. Where: m = 0 for Main or m = 1-4 for Expansion module. (Small Systems, CS 1000S, MG 1000B, and MG 1000T) See "Using the Enable/ Disable commands" in the introduction.	basic-1
DISU BRI l s c	Disable ISDN BRI BRSC card.	brit-19
DISU c d	Disable specified Digital Subscriber Loop (0-7). (Small Systems, CS 1000S, MG 1000B, and MG 1000T). If BRI reference clock source is configured on the DSL, the user will be prompted with: `CLOCK SOURCE ON THIS DSL, PROCEED?`	bri-18
DISU c u	Disables specified unit. See "Using the Enable/Disable commands" in the introduction. (Small Systems, CS 1000S, MG 1000B, and MG 1000T) For Small System: 0-15 may be accepted as input for card 0.	basic-1
DISU l s c d	Disable specified Digital Subscriber Loop 0-7. If BRI reference clock source is configured on the DSL the user will be prompted with: `CLOCK SOURCE ON THIS DSL, PROCEED?`	bri-18
DISU l s c u	Disable specified unit. See "Using the Enable/Disable commands" in the introduction.	basic-1
DIS VTRM <cust> <rout>	Disables all IP Peer Virtual Trunk TNs in the specified route associated with the specified customer and the associated DCIP.	basic-4.00
DLIF c	Download a UIPE BRI trunk interface data file to MISP card (Small System).	bri-18
DLIF l x	Download an UIPE BRI trunk interface data file to a MISP loop. The MISP specified must have the BRIT UIPE loadware application. Where x may be: • (0) = UIPE SL1 • 1 = ETSI QSIG • 2 = ISO QSIG	bri-18

Command	Description	Pack/Rel
	• 28 = ETSI QSIG GF • 29 = ISO QSIG GF To achieve a successful download: 1. the MISP basecode must be enabled 2. the specified MISP must have the UIPE BRI trunk loadware configured 3. the interface must be inactive (interpret this to mean that either the UIPE BRI trunk application must be disabled or no DSL of this interface type can be enabled) 4. QSIG package 263 is required to have ETSI and ISO options.	
DSCT l	Disable automatic background continuity tests for a superloop.	xpe-15
	Where: loop = 0-252 and must be a superloop (multiples of 4), System with Fibre Network Fabric	fnf-25
DSIF L PDL2 l s c	Disables the SAPI 16 interface number for BRSC on l s c for the MPH on loop L.	bri-19
DSIF L PDL2 L1	Disables SAPI 16 interface number for BRIL on Loop L1 for MPH on loop L.	bri-19
DSIF l s c DSL BCH x		bri-19
	Disables the link interface for B-channel x for DSL l s c bch. Where: x = 1–2	
DSIF l s c DSL DCH x		
	Disables the link interface number for USID x for the DSL on l s c dch.	bri-19
DSIF l PDNI Y	Disable the link interface number Y for PDNI on Loop Y (1-3)	bri-19
DSNW l	Disable network card containing specified loop, where "loop" is the number of the even or odd loop. Not applicable to superloops.	basic-1
DSPS x	Disables Peripheral Signaling (PS) card x and loops serviced by the card. Where:	basic-1

<table>
<tr><th>Command</th><th>Description</th><th>Pack/Rel</th></tr>
<tr><td></td><td>• x = 0-9, Option 51C, 61C
• x = 0-15, System with Fibre Network Fabric

Disabling PS card 0 interrupts service on loops 0 to 15. To re-enable the card, use the ENPS x command. If this fails, a system initialization may be required. Use the disable command with discretion. Disabling a PS card disables up to 16 loops.

The following lists the group/PS/loop relationship:

<table><tr><th>Group</th><th>PS</th><th>Loops</th></tr><tr><td>0</td><td>0</td><td>0 to 15</td></tr><tr><td>0</td><td>1</td><td>16 to 31</td></tr><tr><td>1</td><td>2</td><td>32 to 47</td></tr><tr><td>1</td><td>3</td><td>48 to 63</td></tr><tr><td>2</td><td>4</td><td>64 to 79</td></tr><tr><td>2</td><td>5</td><td>80 to 95</td></tr><tr><td>3</td><td>6</td><td>96 to 111</td></tr><tr><td>3</td><td>7</td><td>112 to 127</td></tr><tr><td>4</td><td>8</td><td>128 to 143</td></tr><tr><td>4</td><td>9</td><td>144 to 159</td></tr><tr><td>5</td><td>10</td><td>160 to 175</td></tr><tr><td>5</td><td>11</td><td>176 to 191</td></tr><tr><td>6</td><td>12</td><td>192 to 207</td></tr><tr><td>6</td><td>13</td><td>208 to 223</td></tr><tr><td>7</td><td>14</td><td>224 to 239</td></tr></table></td><td>fnf-25</td></tr>
<tr><td>DSRB c d</td><td>Disable Remote Loop Back for specified BRI Trunk DSL (Small Systems, CS 1000S, MG 1000B, and MG 1000T)</td><td>bri-18</td></tr>
<tr><td>DSRB l s c d</td><td>Disable Remote Loop Back for specified BRI Trunk DSL</td><td>bri-18</td></tr>
<tr><td>DSRM <cust #> <route #></td><td></td><td></td></tr>
<tr><td></td><td>For CS 1000S</td><td>basic-2</td></tr>
</table>

Command	Description	Pack/Rel
	Disables all route members in a customer's route. It will disconnect all active calls associated with the trunks, disable all route members on the call server, unregister all trunks and remove them from the RLM table. On the Signaling Server side, all trunks will be removed from the Signaling Server list. **Note:** Not available for CS 1000 Release 4.0 or later.	
DSTS c d	Disable Remote Loop Back test mode for specified BRI Trunk DSL (Small Systems, CS 1000S, MG 1000B, and MG 1000T)	bri-18
DSTS l s c d	Disable Remote Loop Back test mode for specified BRI Trunk DSL	bri-18
DSXP x	Disable Controller x and all connected cards.	xpe-15
ECNT CARD l s c <customer>		
	For CS 1000S	basic-2
	Prints the number of IP Phones registered for the specified card. If <customer> is specified, the count is specific to that customer (note that a card must be specified to enter a customer.) Otherwise, the count is across all customers. If no parameters are entered, the count is printed for all zones. A partial TN can be entered for the card (L or L S) which then prints the count per that parameter (a customer cannot be specified in this case).	
ECNT NODE nodeNum		
	For CS 1000S	basic-2
	Prints the number of IP Phones registered for the specified node. If no parameter is entered, the count is printed for all nodes.	
ECNT SS <hostName>		
	For CS 1000S	basic-2

Command	Description	Pack/Rel
	Prints the number of IP Phones registered for the specified signaling server. If no parameter is entered, the count is printed for all signaling servers. **Note:** If the hostName variable contains an underscore (_), then an NPR001 error message is returned, as an underscore is considered to be an invalid character.	
ECNT ZONE zoneNum <customer>		
	For CS 1000S	basic-2
	Prints the number of IP Phones registered for the specified zone. If <customer> is specified, the count is specific to that customer. Otherwise, the count is across all customers. If no parameters are entered, the count is printed for all zones.	
ENCT l	Enable automatic background continuity tests for loop.	xpe-15
	Where: • loop = 0-159 • loop = 0-252 and must be a superloop (multiples of 4), System with Fibre Network Fabric	fnf-25
END	Abort current test. Stops outputting. Stops current test.	basic-1
ENIF L PDL2 l s c	bri-19	
	Enables the SAPI 16 interface number for BRSC on l s c for MPH on loop L.	
ENIF l s c DSL BCH x		
	Enables the link interface for B-channel x for DSL l s c bch. Where: x = 1–2	bri-19
ENIF l s c DSL DCH x		
	Enables the link interface number for USID x for the DSL on l s c dch.	bri-19

Command	Description	Pack/Rel
ENIF l PDNI Y	Enables the link interface number Y for PDNI on Loop Y (1-3).	bri-19
ENL AUTO c d	Enable automatic link recovery option of a DSL (Small Systems, CS 1000S, MG 1000B, and MG 1000T)	bri-18
ENL AUTO l s c u	bri-18 Enable automatic link recovery option of a DSL.	
ENLC (appl) c	Enable specified application on Multi-purpose ISDN Signaling Processor (MISP) card. (Small Systems, CS 1000S, MG 1000B, and MG 1000T). Where: appl = optional application name BRIL (Basic Rate Interface Line) or BRIT (Basic Rate Interface Trunk)	bri-18
ENLC (appl) c FDL	bri-18 Enable and force download loadware for specified application on Multi-purpose ISDN Signaling Processor (MISP) card. (Small Systems, CS 1000S, MG 1000B, and MG 1000T). Where: • appl = BRIL (optional application name: Basic Rate Interface Line), or • appl = BRIT (Basic Rate Interface Trunk)	
ENLC (BASE) l s c (FDL/NST)	brit-19 Enable specified card. If the card resides on a disabled shelf, the status is output and enable is not performed. If card has been disabled by overload, the overload status entry is cleared. Used to enable the ISDN Basic Rate Interface Signaling Concentrator (BRSC) card. The command format is shown here. ENLC (BASE) l s c u (FDL/NST) Where: • BASE = enable only the BRSC basecode. If not specified, both the basecode and the application will be enabled. • l = loop • s = shelf • c = card	

Command	Description	Pack/Rel
	• FDL = force download the basecode • NST = No self-test The card faceplate is turned off to indicate the card is enabled, and the IPC channel is built.	
ENLC BRI l s c (FDL)	brit-19 Enable the BRSC ISDN BRI application. Where: • BRI = the BRSC ISDN BRI application • l = loop • s = shelf • c = card • FDL = force download the application The application is force downloaded if: • FDL is entered, or • No application currently exists on the BRSC card, or • There is a version number mismatch between the applications in the software and on the card.	
ENLC c	Enable and reset specified DTR/MFR card. (Small Systems, CS 1000S, MG 1000B, and MG 1000T) If the card resides on a disabled shelf, the status is output and enable is not performed. If card has been disabled by overload, the overload status entry is cleared. This command is also used for Multi-purpose ISDN Signaling Processor (MISP)., S/T-Interface (SILC), and U-Interface (UILC) line cards. This command causes the card to perform a self test. If the card self test passes, the LED will blink 3 times. If it fails, the LED will be lit solidly. A XMI message will be issued to indicate that the XMFR card has powered up. This command can be used to enable a XMFR card. ENLC 0 enables all units (0-15) on TDS card 0 if enabled. The TDS card can be enabled by entering the command ENLX 0 in LD 34.	basic-1
ENLC c FDL	Enable Multi-purpose ISDN Signaling Processor (MISP) and force download basecode.(Small Systems, CS 1000S, MG 1000B, and MG 1000T)	bri-18
ENLC l s c	Enable and reset specified peripheral card.	basic-1

Command	Description	Pack/Rel
	If the card resides on a disabled shelf, the status is output and enable is not performed. If card has been disabled by overload, the overload status entry is cleared. This command causes the card to perform a self test. If the card self test passes, the LED will blink 3 times. If it fails, the LED will be lit solidly. A XMI message will be issued to indicate that the XMFR card has powered up. This command can be used to enable a XMFR card. This command is also used for the S/T-Interface (SILC) and U-Interface (UILC) line cards. For MGX, cards 8,9 and 10 are treated as one card. Issuing a command for card 8 also affects cards 9 and 10. Issuing a command for card 9 also affects card 10. Issuing a command for card 10 only affects card 10.	
ENLG x	Enable group x. Equivalent to two ENPS commands. Refer to DSPS command for the relationships of groups, PS cards and loops.	basic-1
	Where: x = Group 0-7, System with Fibre Network Fabric	fnf-25
ENLL (appl) l	Enable specified application on Multi-purpose ISDN Signaling Processor (MISP) loop. Where: • appl = BRIL (Basic Rate Interface Line), or • appl = BRIT (Basic Rate Interface Trunk)	bri-18
ENLL (appl) l 1	bri-18 Enable MISP application, and loop. Where: • appl = optional application name (BRIL) • loop = loop number • 1 = force download the application	
ENLL (appl) l FDL	bri-18 Enable and force download loadware for specified application on Multi-purpose ISDN Signaling Processor (MISP) loop. Applicable if SUPP package 131 is equipped.	
ENLL (appl) l 1	Enable MISP loop. Where:	bri-18

Command	Description	Pack/Rel
	• appl = optional application name (BRIL) • 1 = force downloads the application • Applicable if SUPP package 131 not equipped.	
ENLL l	Enable network loop. See "Using the Enable/Disable commands" in the introduction. This command is also used for Multi-purpose ISDN Signaling Processors (MISP).	basic-1
ENLL l FDL	Enable MISP and force download basecode.	bri-18
ENLL l (v)	Enable superloop, download peripheral software version v. If version v is not specified, the software downloaded is current (c) or latest (l) version as defined in LD 97.	xpe-15
ENLL sl	Enable specified Superloop. OK is output if the operation is successful.	basic-21
ENLR c u	Enable the specified DTR/MFR card. (Small Systems, CS 1000S, MG 1000B, and MG 1000T) System software will issue a message to request XMFR to perform an echo test only when ENLR is issued to enable the XMFR card.	basic-21
ENLR l s c u	Enable the specified DTR/MFR card. System software will issue a message to request XMFR to perform an echo test only when ENLR is issued to enable the XMFR card. **Note:** This is a Small Systems, CS 1000S, MG 1000B, and MG 1000T specific command.	basic-21
ENLS l s	Enable specified shelf. Where: l = loop and s = shelf. If the shelf is disabled by overload, the overload status entry is cleared.	basic-1
ENLS m	Enable the specified module. (Small Systems, CS 1000S, MG 1000B, and MG 1000T). Where: m = 0 for base module or m = 1-4 for expansion module. If the module is disabled by overload, the overload status entry is cleared.	basic-1
ENLU c d	Enable Digital Subscriber Loop (0-7) (Small Systems, CS 1000S, MG 1000B, and MG 1000T)	bri-18

Command	Description	Pack/Rel
ENLU c u	Enable specified unit. (Small Systems, CS 1000S, MG 1000B, and MG 1000T) ENLU c u accepts units 0-15 as input. Units can only be enabled if TDS 0 is enabled. **Note:** For Slot 0, the TDS must first be enabled by entering the command ENLX 0 in LD 34 (Small Systems, CS 1000S, MG 1000B, and MG 1000T).	basic-1
ENLU l s c d	Enable Digital Subscriber Loop (0-7).	bri-18
ENLU l s c u	Enable specified unit. If the unit resides on a disabled shelf or card, the status is output and enable is not performed. If the unit to be enabled is a 500/2500 message waiting telephone, test the unit prior to enabling.	basic-1
ENL VTRM <cust> <rout>	basic-4.00 Enables all IP Peer Virtual Trunk TNs in the specified route associated with the specified customer and the associated DCIP.	
ENNW l	Enable network card with specified loop, where loop is the even or odd numbered loop on the network card. Not applicable to superloops.	basic-1
ENPS x	Enables PS card x and all loops that were enabled at time of last DSPS command. Refer to DSPS command to find the relationships of groups, PS cards and loops. Where: x = 0-15, Enable PS card and clear PBX_LAMP BADBITS for System with Fibre Network Fabric	basic-1 fnf-25
ENRB c d	Enable Remote Loop Back for specified BRI Trunk DSL. (Small Systems, CS 1000S, MG 1000B, and MG 1000T)	bri-18
ENRB l s c d	Enable Remote Loop Back for specified BRI Trunk DSL.	bri-18
ENRM <cust #> <route #>	For CS 1000S Enable all the virtual trunk route members in a customer's route. It will enable all route members, register them and put them into the RLM table. On the Signaling Server side, all trunks will be put on the Signaling Server list.	basic-2

Command	Description	Pack/Rel
	Note: Not available for CS 1000 Release 4.0 or later.	
ENTS c d	Enable Remote Loop Back test mode for specified BRI Trunk DSL. (Small Systems, CS 1000S, MG 1000B, and MG 1000T)	bri-18
ENTS l s c d	Enable Remote Loop Back test mode for specified BRI Trunk DSL.	bri-18
ENXP x (v)	Enable Controller x and associated IPE cards, download software version v. Enable all IPE cards connected to Controller x and the Controller itself. If version v is not specified, the software downloaded to the Controller is current (c) or latest (l) version as defined in LD 97.	xpe-15
ENXP XPC x (v)	Enable Controller x, do not enable the associated IPE cards, download software version v. The cards connected to the Controller are not enabled by this command. If version v is not specified, the software downloaded to the Controller is current (c) or latest (l) version as defined in LD 97.	xpe-15
ESTU c d	Establish D-channel link for the specified Digital Subscriber Loop (0-7). (Small Systems, CS 1000S, MG 1000B, and MG 1000T)	bri-18
ESTU l s c d	Establish D-channel link for the specified Digital Subscriber Loop (0-7).	bri-18
FDIS NCAL <c DSL#> <conn_id>	qsig gf-22 Force disconnect the specified call-independent connection (as defined by its connection ID number) Note that the command format for an Small Systems, CS 1000S, MG 1000B, and MG 1000T is: `STAT NCAL <c 0 0 DSL#><conn_id#>`	
FDIS NCAL <l s c DSL#> <conn_id>	qsig gf-22 Force disconnect the specified call-independent connection (as defined by its connection ID number)	

Command	Description	Pack/Rel
FDLC	Cancel or stop the sytem wide flash download for M39xx units. Units include: M3902, M3903, M3904 and M3905.	arie- 25
FDLF l s c u	Initiate forced download to one M39xx unit regardless of version or state. Units include: M3902, M3903, M3904 and M3905.	arie- 25
FDLI l s c u	Initiate download to one M39xx unit when the set becomes idle, if the set's firmware is not current. Units include: M3902, M3903, M3904 and M3905.	arie- 25
FDLU l s c u	Initiate download to one M39xx unit, if the set's firmware is not current. Units include: M3902, M3903, M3904 and M3905.	arie- 25
FDLS	Initiate system wide flash download according to the FDL schedule programmed in Overlay 97	arie- 25
FSUM	Print summary report of firmware versions currently on M39xx units. Units include: M3902, M3903, M3904 and M3905.	arie- 25
FSUM ALL	Print complete report of all M39xx sets based on parameters specified in LD 97.	arie-25
FWVU l s c u	Query and print the firmware versions currently on M39xx terminal.	arie- 25
IDC c	Print MISP or IPE card ID. (Small Systems, CS 1000S, MG 1000B, and MG 1000T) The MISP card ID output format is: • CARDID: xxx. . . x • BASECODE VERSION: xxx. . . x • BRI LINE/TRUNK VERSION: xxx. . . x • BOOTCODE VERSION: xxx. . . x The MISP card ID output format is: • CARDID: xxx. . . x • BASECODE VERSION: xxx. . . x • BRI LINE/TRUNK VERSION: xxx. . . x • BOOTCODE VERSION: xxx. . . x	bri-18
IDC l	Print ID of Network and Peripheral Controller	fnf-25

Command	Description	Pack/Rel
	Where: l = 0-252 and must be a superloop (multiple of 4), System with Fibre Network Fabric.	
IDC l s c	Print BRSC card and loadware version. This command, queries the BRSC card ID, the basecode, and the application version number. Where: l = loop, s = shelf, and c = card. Output example: • BOOTCODE VERSION xx . . . x • BASECODE VERSION xx . . . x • BRI APPL VERSION xx . . . x	brit-19
IDC l s c	Print MISP or IPE card ID. The MISP card ID output format is: • CARDID: xxx. . . x • BASECODE VERSION: xxx. . . x • BRI LINE/TRUNK VERSION: xxx. . . x • BOOTCODE VERSION: xxx. . . x The IPE card ID output format is: `=> XXXX CCCCCCCC-RRSSSS` Where: • XXXX = card type (i.e., XDTR, XUT, etc.) • CCCCCCCC = order code • RR = release number • SSSS = is the serial number	bri-18
IDC l s c d	Print ID of Digital Subscriber Loop 0-7.	bri-18

IDC sl	For Copper Connections
	Print Network ID and Controller for a superloop.
	Output format for superloop card ID:
	`XNET VERS => xxx`
	`RUNNING FROM yyy`
	`FW IS SANE`
	`CCCCCCCC-RRSSSS`
	`XPEC0 VERS => xxx`
	`RUNNING FROM yyy`
	`FW IS SANE`
	`XPECz CCCCCCCC-RRSSSS`
		xpe-15

Command	Description	Pack/Rel
	XPEC1 VERS => xxx RUNNING FROM yyy FW IS SANE XPECz CCCCCCCC-RRSSSS Where: • xxx = loadware version • yyy = RAM or ROM • z = 2 or 4 • CCCCCCCC = order code • RR = release number • SSSS = is the serial number	
IDC sl	For Carrier Connections Get card id of Local Carrier Interface (LCI) superloop and its associated Remote Carrier Interface (RCI). Output format for LCI superloop card ID: LCI VERS => xxx FW IS SANE aaaaaaaaaaaa Output format for RCI superloop card ID: XPEC VERS=>xxx FW IS SANE aaaaaaaaaaaa Where: • xxx = loadware version • aaaaaaaaaaaa = contents of ID EEPROM (LCI or RCI)	rem_ipe-21
IDC sl	For Fiber Connections Print card ID of optical packets and main boards for Fiber superloop and associated Controller(s). The output format for the superloop card ID including optical packets is: FNET VERS => xxx FW IS SANE aaaaaaaaaaaa PRIM: pppppppp SEC: ssssssss XPEC VERS => xxx FW IS SANE aaaaaaaaaa	rem_ipe-22

Command	Description	Pack/Rel
	PRIM: pppppppp SEC: ssssssss Where: 1. xxx = loadware version 2. aaaaaaaaaaaa = contents of ID EEPROM (FNET or FPEC) 3. PRIM: pppppppp = contents of ID EEPROM primary packet (if present) 4. SEC: ssssssss = contents of ID EEPROM secondary packet (if present)	
IDC l s c	Print card ID for IPE card. The format is: IDC l s c — print ID of specified line card The format of the card ID is CCCCCCCC-RRSSSS , where: • CCCCCCCC = order code • RR = release number • SSSS = serial number For example, a Network Card (NT8D04AA) with a release of 01 and serial number of 00001 will have a card ID with: NT8D04AA-010001 For BRI MISP cards, the output is: • CARDID: xxx...x • BASECODE VERSION: xxx...x • BRI LINE/TRUNK VERSION: xxx...x • BOOTCODE VERSION: xxx...x	xpe-15
IDCS x	Print card ID for all cards on shelf controlled by Controller x. The card ID for all cards in shelf controlled by Controller x is output. The IPE card ID output format is: => XXXX CCCCCCCC-RRSSSS Where: • XXXX = card type (i.e., XDTR, XUT, etc.) • CCCCCCCC = order code • RR = release number • SSSS = is the serial number	xpe-15

Command	Description	Pack/Rel
IDU c d	Print set ID for Digital Subscriber Loop d (0-7) (Small Systems, CS 1000S, MG 1000B, and MG 1000T)	bri-18
IDU l s c d c u	Print set ID for Digital Subscriber Loop d (0-7) Small Systems, CS 1000S, MG 1000B, and MG 1000T format	bri-18
IDU l s c u	Print set ID. Print ID applies to the following set types: M2006, M2008, M2016, M2216 and M2616. The output format of the set ID (M2008 for example) is: • ARIES TN: l s c u • TN ID CODE: M2008 • NT CODE: NT2K08WC • COLOR CODE: xx • RLS CODE: xx • SER NUM xxxxxx The color codes are: • 03 is black • 35 is chameleon ash • 93 is dolphin grey	xpe-15
IDU <TN>	Prints the MAC address, Model Vendor, software version, Set IP address.	basic-3.0
LBD l s	List TN of all PBX units on specified shelf, with lamps flagged as defective.	fnf-25
LBSY l s	List TNs of all busy units on specified shelf.	basic-1
LBSY m	List TNs of all busy units in specified module. (Small Systems, CS 1000S, MG 1000B, and MG 1000T). Where: m = 0 for Base module or 1 for Expansion module.	basic-16
LDIS l s	List TNs of all disabled units on specified shelf.	basic-1
LDIS m	List TNs of all disabled units on specified module. (Small Systems, CS 1000S, MG 1000B, and MG 1000T). Where: m = 0 for Base module or 1 for Expansion module.	basic-16
LIDL l s	List TNs of all idle units on specified shelf.	basic-1

Command	Description	Pack/Rel
LIDL m	List TNs of all idle units in specified module. (Small Systems, CS 1000S, MG 1000B, and MG 1000T). Where: m = 0 for Base module or 1 for Expansion module.	
LMNT l s	List TNs of all maintenance busy units on specified shelf.	basic-1
LMNT m	List TNs of all maintenance busy units on specified module. (Small Systems, CS 1000S, MG 1000B, and MG 1000T). Where: m = 0 for Base module or m = 1 for Expansion module.	
PBXH	Message Waiting lamp maintenance.	basic-1
PBXT (c u), ALL	Tests 500/2500 Message Waiting lamp on specified card or unit. This is required after failed lamp is fixed. (Small Systems, CS 1000S, MG 1000B, and MG 1000T)	basic-1
PBXT ALL	Test all Message Waiting lamps on 500/2500 telephones on all loops	basic-5
	Where: ALL = loops 0-255, System with Fibre Network Fabric	fnf-25
PBXT l (s c u)	Tests 500/2500 Message Waiting lamp on specified loop, shelf, card or unit. This is required after failed lamp is fixed.	basic-5
PCON c d	Upload and print configuration and LAPD parameters for specified DSL. (Small Systems, CS 1000S, MG 1000B, and MG 1000T)	bri-18

PCON l s c d	Upload and print configuration and LAPD parameters for specified DSL. This command requires the specified DSL to be configured for the BRI Trunk Application. See example below:
	`PCON 6 0 0 6`
	`.DSL: 6 0 0 6 LINL PARAM CONFIRM TIME: 0:02:10`
	`INTERFACE: SL-1`
	`OPER MODE: USR`
	`T200: 2`
	`T203: 20`
	`N200: 3`
	`N201: 260`
	`K: 1`
	`PROT #: 1`
		bri-18

Command	Description	Pack/Rel
PERR (appl) c	Upload and print Layer 2 error log for specified SILC, UILC or MISP card. (Small Systems, CS 1000S, MG 1000B, and MG 1000T) Where (appl): • BRIE for UIPE Basic Rate Interface Trunk • BRIT for NON-UIPE Basic Rate Interface Trunk	bri-18
PERR (appl) l	Upload and print Layer 2 error log for specified MISP. Where (appl): • BRIE for UIPE Basic Rate Interface Trunk • BRIT for NON-UIPE Basic Rate Interface Trunk	bri-18

PERR (appl) l s c	Upload and print Layer 2 error log for specified SILC or UILC. This command requires the specified MISP or line card to be configured for the BRIT Application.
	Where (appl):
	• BRIE for UIPE Basic Rate Interface Trunk
	• BRIT for NON-UIPE Basic Rate Interface Trunk
	If error log is requested for a line card the error log for each DSL is printed. If error log is requested for a MISP the application global log is also printed.
	Interpretation of error logs:
	1st byte is DSL number or "80" for Application log. 2nd byte is number of non-zero logs.
	If errors were logged the subsequent information is printed for each error type:
	• 3rd byte is counter type code
	• 4th byte is "HIGH" byte of count
	• 5th byte is "LOW" byte of count
	Examples follow :
	`PERR brie 6`
	`.DSL: 6 0 0 6 ERR LOG CONFIRM TIME: 0:02:10`
	`00 00 01 00 06 00 07 00`
	`^ ^ ^ ^`
	`DSL 0 DSL 1 DSL 6 DSL 7 (no errors for all DSLs)`
	`PERR brie 3`
		bri-18

Command	Description	Pack/Rel
	.DSL: 5 0 0 2 ERR LOG CONFIRM TIME: 0:02:10 80 01 4D 00 09 Where: • 1st byte - 80 - indicates Application global log • 2nd byte - 01 - is number of error logs • 3rd byte - 4D - is counter type code • 4th bye - 00 - is "HIGH" byte count • 5th byte - 09 - is "LOW" byte counts for all DSLs	
PLOG c d	Upload and print protocol log for specified BRI Trunk DSL. (Small Systems, CS 1000S, MG 1000B, and MG 1000T)	bri-18
PLOG l s c d	Upload and print protocol log for specified BRI Trunk DSL. The protocol log keeps record of up to 32 protocol types. Only non-zero counters are uploaded and printed. This command requires the specified MISP or line card to be configured for the BRIT Application. See example below: PLOG 6 0 0 6 .DSL: 6 0 0 6 PROTOCOL CONFIRM TIME: 0:02:10 17 117 <--Counter 17 shows 117 SABME frames received with incorrect C/R bit 18 141 <--Counter 18 shows 141 supervisory frames received with F=1 19 84 <--Counter 19 shows 84 unsolicited DM responses with F=1	bri-18
PMES c d	Upload and print Layer 3 message log for specified DSL. (Small Systems, CS 1000S, MG 1000B, and MG 1000T)	bri-18
PMES l s c d	Upload and print Layer 3 message log for specified DSL. This command requires the specified DSL to be configured for the BRI Trunk Application. Each time a valid Layer 3 message is received by the MISP, a counter for that particular message is incremented. The log keeps track of up to 20 message types. Only non-zero items are uploaded and printed. Making trunk calls will create a printable log. In the following example, 2 calls were made: PMES 6 0 0 6 .DSL: 6 0 0 6 MSG LOG CONFIRM TIME: 0:02:10 ALERT: 2 PROC: 2 CONNECT: 2	bri-18

Command	Description	Pack/Rel
	DISCONN: 2 REL COP: 2	
PTAB c d	Upload and print Layer 3 Message configuration IE table for specified BRI trunk DSL. (Small Systems, CS 1000S, MG 1000B, and MG 1000T)	bri-18
PTAB l s c d	Upload and print Layer 3 Message configuration IE table for specified BRI trunk DSL. PTAB uploads what was downloaded when the Application was enabled.	bri-18
PTAB c d <tbl #>	Upload and print specified Layer 3 Message configuration IE table for specified BRI trunk DSL. Where: <tbl #> = table number. (Small Systems, CS 1000S, MG 1000B, and MG 1000T)	bri-18
PTAB l s c d <tbl #>	Upload and print specified Layer 3 Message configuration IE table for specified BRI trunk DSL. PTAB uploads what was downloaded when the Application was enabled. Where: <tbl #> = table number.	bri-18
PTRF c d	Upload and print traffic report for specified BRI Trunk DSL. (Small Systems, CS 1000S, MG 1000B, and MG 1000T) The following traffic information is output: CONNECTED NCALLS : Total number of established call-independent connections	bri-18
PTRF l s c d	Upload and print traffic report for specified BRI Trunk DSL. This command requires the specified DSL to be configured for the BRI Trunk Application. See example below: PTRF 6 0 0 6 .DSL: 6 0 0 6 TRAFFIC CONFIRM TIME: 0:02:10 PEAK_I_US: 0 <-- Peak link usage (over a 5 second period) for incoming traffic since the last time the traffic data was uploaded. An integer 0 - 100 which represents the percentage of the link capacity used. AVRG_I_US: 0 <-- Average link usage for incoming traffic since the traffic was last uploaded. PEAK_O_US: 0 <-- Peak link usage (over a 5 second period) for outgoing traffic since the last time the traffic	bri-18

Command	Description	Pack/Rel
	data was uploaded. An integer 0 - 100 which represents the percentage of the link capacity used. AVRG_O_US: 0 <-- Average link usage for outgoing traffic since the traffic was last uploaded. TIME: 0 <-- time since last traffic upload query CONNECTED CALL: 2 <-- number of successfully connected trunk calls	
RLBT c d	Perform Remote Loop Back Test on specified BRI Trunk DSL. (Small Systems, CS 1000S, MG 1000B, and MG 1000T)	bri-18
RLBT l s c d	Perform Remote Loop Back Test on specified BRI Trunk DSL.	bri-18
RLSU c d	Release D-channel link for specified Digital Subscriber Loop (0-7). (Small Systems, CS 1000S, MG 1000B, and MG 1000T)	bri-18
RLSU l s c d	Release D-channel link for specified Digital Subscriber Loop (0-7).	bri-18
RMIF L PDL2 l s c	bri-19 Disables and removes the SAPI 16 interface number for BRSC on l s c for MPH on loop L.	
RMIF L PDL2 L1	Disables and removes the SAPI 16 interface number for BRIL on Loop L1 for MPH on loop L.	bri-19
RMIF l s c DSL BCH x	bri-19 Disables and removes the link interface for B-channel x for DSL l s c bch; where: x = 1–2	
RMIF l PDNI Y	Disables and removes the link interface number Y for PDNI on Loop Y (1-3)	bri-19
STAT	Get status of all configured loops in system	basic-1
STAT (appl) c	Get status of MISP card and application. (Small Systems, CS 1000S, MG 1000B, and MG 1000T) See STAT (appl) loop for possible responses.	bri-18

Command	Description	Pack/Rel
STAT (c)	Get status of all cards or (specified card). (Small Systems, CS 1000S, MG 1000B, and MG 1000T) See STAT (loop) and STAT l s c for possible responses. STAT 0 provides the status of TDS 0 and units 0-15 for card 0.	basic-1
STAT c d	Get status of specified DSL. (Small Systems, CS 1000S, MG 1000B, and MG 1000T) See STAT l s c d for possible responses.	bri-18
STAT c u	Get status of specified unit. For Small System For CS 1000S STAT c u accepts units 0-15 as input for card 0. Refer to STAT l s c u for additional output examples IP Phone registration and login status. The response format is x[y[z]] Output Example: x, y, Login Status Where: x = • IDLE • BUSY • UNEQ • DSBL y = • REGISTERED • UNREGISTERED • LOCAL REGISTERED • LOCAL UNREGISTERED z = • 0 - Initialize status • 1 - Branch User Login • 2 - Branch User Local Mode Test • 3 - Branch User Config • 5 - Branch User Forced Logout (F/W Download) • 6 - Branch User No Branch Password Provisioned • 7 - Branch User Locked from Branch Password Retry • 8 - Branch User No Main Password Provisioned • 9 - Branch User Locked from Main Password Retry	basic-1 basic-2

Command	Description	Pack/Rel
	• 10 - Branch User Gatekeeper Unreachable • 11 - Branch User ID unrecognized by Gatekeeper • 12 - Branch User Main Office TPS Unreachable • 13 - Branch User ID - TN combination unrecognized by Main Office Call Server • 14 - Branch User Firmware Out of Sync • 30 - Virtual Office Login • 32 - Virtual Office Locked from Login	
	With release 4.5 Active Call Failover status is output as: ACF STATUS <status> TMR <timer> • where status is: - UNREG for unregistered calls - HREG for half-registered calls - HREB for half-rebuilt calls - REB for rebuilt calls - PREB for partially-rebuilt calls • where <timer> is: - an integer value if the timer exists for the call - N/A if there is no Call Server ACF timer attached	basic-4.50
	STAT command example output .stat 81 1 BUSY UNREGISTERED 00 ACF STATUS UNREG TMR 110 .stat 81 2 BUSY REGISTERED 00 ACF STATUS HREG TMR N/A .stat 81 3 BUSY REGISTERED 00 ACF STATUS REB TMR N/A	basic-4.50

STAT (appl) l	Get status of MISP loop and application.
	If appl = BRIL, the status of the BRI Line application is output. If appl = BRIT, the status of the BRI Trunk application is output.
	Typical response is:
	`loop` = MISP loop for Large System and CS 1000E System
	`mm DSBL nn BUSY`
	`MISP lll : ENBL ACTIVATED timestamp`
	`BRIL : ENBL`
	`BRIT :  ENBL`
	If the card has been manually disabled, the response is:
		bri-18

Command	Description	Pack/Rel

`loop` = MISP loop for Large System and CS 1000E System

```
DISABLED RESPONDING
MAN DSBL
```

If the card has been disabled by the system, the response is:
`loop` = MISP loop for Large System and CS 1000E System

```
DISABLED RESPONDING
SYS DSBL - aaa...a
```

Where aaa...a is the reason as follows:

1. `BOOTLOADING` = basecode is being downloaded to the MISP
2. `FATAL ERROR` = MISP has a serious problem
3. `OVERLOAD` = MISP overload (card inoperable)
4. `RESET THRESHOLD` = too many resets (card inoperable)
5. `SELF TESTING` = card is performing self-test
6. `SELFTEST FAILED` = self-test failed
7. `SELFTEST PASSED` = successfully completed self-test
8. `SHARED RAM TEST FAILED` = MISP memory problem (card inoperable)
9. `STUCK INTERRUPT` = MISP hardware failure (replace card)

With the STAT BRIL or STAT BRIT option, the response is one of the following:

- `APPLICATION ENBL`
- `APPLICATION NOT CONFIGURED`
- `APPLICATION NOT RESPONDING`
- `APPLICATION MAN DSBL` (manually disabled)
- `APPLICATION SYS DSBL - aaa..a` (system disabled)

Where aaa...a is the reason as follows:

Command	Description	Pack/Rel
	1. CLOSED = application is closed by basecode on the card 2. CLOSED ERR = error in closing the application 3. CORRUPTED = application is corrupted on the card 4. DOWNLOADING = application is being downloaded 5. ENABLED = application is in active state 6. INACTIVE = application is in inactive state 7. MNT BUSY = application is in maintenance busy state 8. WAIT DSBL = application is in process of being disabled 9. WAIT ENABLE = application is in process of being enabled 10. WAIT ERASE = application is being erased from the card 11. WAIT REMOVE = application is being removed from the card	
STAT (l)	Give status of one or all loops. Response is one of the following: 1. x BUSY, y DSBL = loop enabled with x channels busy and y channels disabled. 2. UNEQ = loop unequipped. 3. CTYF: l1 l2 = loop specified in STAT command is unable to receive data from loops l1, l2, etc. (i.e., continuity test failed in most recent LD 45 loop test). Probable fault in network card. 4. DSBL: NOT RESPONDING = loop disabled. Network card not responding. Card missing, disabled by switch or faulty. 5. DSBL: RESPONDING = loop disabled but the network card responds. Loop may have been disabled due to: a. manual request (DISL) b. associated Peripheral Signaling card being disabled c. overload condition on associated loop	basic-1

Command	Description	Pack/Rel
	Note: Overload conditions are indicated by OVD messages. An attempt to enable a loop which was disabled due to overload may result in a recurrence of the overload condition: the system's service may be impaired for about 2 minutes. **Note:** For MISP loops see STAT (appl) loop command.	
STAT l s	Get idle, busy or disabled status of units on specified shelf. Displays number of units idle, busy, disabled and maintenance busy for the specified shelf.	basic-1

STAT l s c	Get status of any specified IPE card. (e.g., digital line, analog, DTR, etc.)
	When getting the status of a card relating to a trunk error (STAT), the term RVSD may appear with the trunk information. RVSD indicates that the software has detected a reversed wired trunk for that unit.
	When getting the status of a card where ACD sets are defined, the printout will include MSB LOG OUT, MSB LOG IN, LOG IN, OR LOG OUT, according to the ACD set state.
	The output format for either a S/T-Interface line card (SILC) or an U-Interface line card (UILC) is:
	For BRI trunks:
	`ll` = UNIT ll = DSL/UNIT number on the card =
	`swstate type L2_state L1_state dch_state clk (mode)`
	For BRI lines:
	`ll` = UNIT ll = DSL/UNIT number on the card =
	`swstate type L2_state L1_state`
	If you are analyzing a SILC or an UILC card, Table 9: STAT l s c Field and Response Definitions on page 122 lists and defines output fields and field responses. For an example of output, see Output Example: on page 122.
		bri-18

	The output format for an `ISDN BRI card` is: loop = `UNIT sw_state DSL misp_state LC_state` With ISDN BRI BRSC cards, the basecode and application status are output.	brsc/basic-19

Command	Description	Pack/Rel

```
APPLICATION     MAIN STATE     SUB STATE/ACTIVATION
   TIME
 +-------------------+-----------------------+-----------------------------------+
 BASECODE        ENABLED              xx/xx/xx x:xx
 BRI               ENABLED              xx/xx/xx x:xx
 +-------------------+-----------------------+-----------------------------------+
   IDLE 0           BUSY 0            DISABLED 8
MSBY 0
   TOTAL DSLS CONFIGURED 8
```

If you are analyzing an ISDN BRI card , see "STAT l s c d" command for a list of possible states.

Output Example:

```
00 = UNIT 00 = IDLE LINE   ESTA UP
01 = UNIT 01 = IDLE TRNK  ESTA UP         ESTA SREF (TE)
02 = UNIT 02 = IDLE LINE   ESTA DOWN
03 = UNIT 03 = UNEQ
04 = UNIT 04 = UNEQ
05 = UNIT 05 = UNEQ
06 = UNIT 06 = DSBL TRNK DSBL UNEQ RLS                (NT)
7 = UNIT 07 = DSBL TRNK DSBL UNEQ RLS               (TE)
```

Table 9: STAT l s c Field and Response Definitions

Field	Field Definition	Response	Response Definition
swstate	state of DSL/UNIT in software	IDLE	no active call
		BUSY	active with a call
		UNEQ	unequipped
		MBSY	maintenance busy
type	DSL type	LINE	BRI line
		TRNK	BRI trunk
L2_state	Layer 2 state of DSL/UNIT in MISP loadware	UNEQ	unequipped
		IDLE	no active call
		BUSY	active with a call
		MBSY	maintenance busy
		DSBL	disabled
		ESTA	D-channel link is established

Field	Field Definition	Response	Response Definition
		RLSU	D-channel link is released
		TEST	test mode
		RLBT	remote loop back
		APDB	application disabled
		MPDB	associated MISP disabled
		MPNR	associated MISP not responding
		UTSM	unable to send message to MISP
L1_state	Layer 1 state of line card	UNEQ	unequipped
		DOWN	Layer 1 is down
		LCNR	line card not responding
		UP	Layer 1 is up
		UNDN	undefined DSL state
		XPDB	Associated XPEC is disabled
		UTSM	unable to send message to MISP
dch_state	State of D-channel link in software	ESTA	D-channel link is established
		RLSU	D-channel link is released
		TEST-IDLE	test mode idle
		TEST-RLBT	test mode remote loop back
clk	Clock mode	DSBL	disabled
		PREF	primary reference
		SREF	secondary reference
mode	Layer 1 mode of DSL	NT	Network Termination
		TE	Terminal Equipment

STAT l s c d Get status of specified Digital Subscriber Loop (0-7). bri-18

When getting the status of an unit where ACD sets are defined, the printout will not include MSB LOG OUT, MSB LOG IN, LOG IN, OR LOG OUT, according to the ACD set state.
If SUPP package 131 is not equipped, Tthe output format is:

```
DSL sw_state misp_state lc_state B1 status
B2 status
```

If SUPP package 131 is equipped, the output format is:

```
DSL type: swstate L2_state L1_state
dch_state clk b1_state b2_state
```

Table 10: STAT l s c d Field Definitions on page 124 defines output fields. Table 11: STAT l s c d Response Definitions: SUPP package 131 is not equipped on page 125 lists and defines possible responses when SUPP package 131 is not equipped. Table 12: STAT l s c d Response Definitions when SUPP package 131 is equipped on page 125 lists and defines possible responses when SUPP package 131 is equipped.

Table 10: STAT l s c d Field Definitions

Field	Definition
sw_state	DSL software state
misp_state	DSL state on the MISP card
lc_state	DSL state on the BRI line card
swstate	State of DSL/UNIT in software
L2_state	Layer 2 state of DSL/UNIT in MISP loadware
L1_state	Layer 1 state of line card
dch_state*	State of D-channel link in software
clk*	Clock mode
b1_state	State of first B-channel
b2_state	State of second B-channel
* these fields are output only for BRI trunks	

Table 11: STAT l s c d Response Definitions: SUPP package 131 is not equipped

Response	Definition
APDB	MISP call application is disabled
BUSY	Call is active
DOWN	Link layer is not established
DSBL	DSL is disabled
ESTA	Link layer is established
IDLE	No active calls
LCNR	Line card is not responding
MBSY	DSL is in maintenance busy mode
MPDB	MISP is disabled
MPNR	MISP not responding or message is lost
NTAN	DSL is not assigned to a MISP
RLS	Link layer is not established
UNDN	DSL is in an undefined state
UNEQ	Unequipped
UP	Link layer is established
UTSM	CPU is unable to send message to MISP or line card
XTDB	Superloop is disabled
XPDB	Controller is disabled

Table 12: STAT l s c d Response Definitions when SUPP package 131 is equipped

Field	Response	Definition
type	LINE	BRI line
	TRNK	BRI trunk
swstate	IDLE	no active call
	BUSY	active with a call
	UNEQ	unequipped
	MBSY	maintenance busy
L2_state	UNEQ	unequipped

Field	Response	Definition
	IDLE	no active call
	BUSY	active with a call
	MBSY	maintenance busy
	DSBL	disabled
	ESTA	D-channel link is established
	RLSU	D-channel link is released
	TEST	test mode
	RLBT	remote loop back
	APDB	application disabled
	MPDB	associated MISP disabled
	MPNR	associated MISP not responding
	UTSM	unable to send message to MISP
L1_state	uneq	unequipped
	DOWN	Layer 1 is down
	LCNR	line card not responding
	UP	Layer 1 is up
	UNDN	undefined DSL state
	XPDB	associated XPEC is disabled
	UTSM	unable to send message to MISP
dch_state	ESTA	D-channel link is established
	RLSU	D-channel link is released
	TEST-IDLE	test mode idle
	TEST-RLBT	test mode remote loop back
clk	DSBL	disabled
	PREF	primary reference
	SREF	secondary reference
b1_state	UNEQ	unequipped
	BUSY	active with a call

Field	Response	Definition
	DSBL	disabled
	MBSY	maintenance busy
	IDLE	no active call
b2_state	UNEQ	unequipped
	BUSY	active with a call
	DSBL	disabled
	MBSY	maintenance busy
	IDLE	no active call

STAT l s c u Get status of specified unit. Table 13: STAT lscu responses on page 127 defines possible responses to STAT lscu. basic-1

Table 13: STAT lscu responses

Type	Response	Definition
Normal	IDLE	Idle
	IDLE REGISTERED	IP Phone is registered.
	IDLE UNREGISTERED	IP Phone is not registered.
	MBSY	Maintenance busy
	DSBL	Disabled
	DSBL	Virtual terminal disabled by Server
	DSBL REGISTERED	IP Phone is registered, but is disabled.
	DSBL UNREGISTERED	IP Phone is not registered and is disabled.
	BUSY	In use by call processing
	BUSY BARRED	Barring is applied to trunk with BARA Class of Service
	UNEQ	Terminal not defined in software
	L500	Line is 500/2500 type
	W500	Line is DECT/MCMO type
	DCS	Digital cordless set

Type	Response	Definition
	DMC	DECT mobility card
	MBCS	Maintenance set
	BCS	Normal SL-1 telephone
	TRK	Trunk
	ATTN	Attendant console
	DTR	Digitone Receiver
	PWR	Console power unit
Abnormal	CARD x DSBL (OVD)	Card x disabled due to overload
	DND xxx xxx	Do Not Disturb feature is active
	SHELF DSBL(OVD)	Shelf disabled due to overload
	SIG FAULT	Outgoing signal fault detected on PS card under examination.
	WARNING: CRPTR NOT IN RANGE	TN's data is corrupted. Check BUG messages relating to the TN.
Responses caused by invalid equipment choice:		
	EXT DSBL	Extender disabled
	LOOP NOT TERM	Loop is not a terminal loop
	LOOP UNEQ	Loop is unequipped
	SHELF UNEQ	Shelf is unequipped
	SHELF UNEQ W/ PBX CARDS	No 500 cards on shelf
	CARD UNEQ	Card is unequipped
	CARD NOT PBX	Card is not a PBX card
	UNIT UNEQ FOR MW	Unequipped for Message Waiting
	PER UNEQ	PS card is unequipped
	UNIT UNEQ	Unit is unequipped

STAT NCAL <c DSL#> qsig gf-22

List all current call-independent connections on a given BRI DSL. (Small System)

Note:
This is applicable for UIPE protocol-based DSLs only, for which the CS 1000 supports call-independent connections ("GF capability").

The response format is as follows:

- `NCALL CONN ID` : a number in the range of 1-9999 that identifies the call independent connection on a given DSL
- `CREF` : call reference number in HEX identifying independent connection
- `STATE` : current state of all call-independent connections (`IDLE` , `CONN_REQ` , `CONN_EST`)
- `TIME` : year month day hour:minute:second (the time when call independent connection request is made)
- `APPL` : applications using the call-independent connection (e.g., NACD, NMS,...)
- `ORIG` : originator
- `DEST` : destination

The command format for a Small System is:
`STAT NCAL <c 0 0 DSL#>`
To receive information from this command, "GF capability" is required. The QSIG protocols require QsigGF package 305. EuroISDN protocols, for which the CS 1000 supports GF transport, support a smaller set of features, but do not require the QsigGF package.

STAT NCAL <l s c DSL#> qsig gf-22

List all current call-independent connections on a given BRI DSL.

Note:
This is applicable for UIPE protocol-based DSLs only, for which the CS 1000 supports call-independent connections ("GF capability").

The response format is as follows:

- `NCALL CONN ID` : a number in the range of 1-9999 that identifies the call independent connection on a given DSL
- `CREF` : call reference number in HEX identifying independent connection

- STATE : current state of all call-independent connections (IDLE, CONN_REQ, CONN_EST)
- TIME : year month day hour:minute:second (the time when call independent connection request is made)
- APPL : applications using the call-independent connection (e.g., NACD, NMS,...)
- ORIG : originator
- DEST : destination

To receive information from this command, "GF capability" is required. The QSIG protocols require QsigGF package 305. EuroISDN protocols, for which the CS 1000 supports GF transport, support a smaller set of features, but do not require the QsigGF package.

STAT NCAL <l s c DSL#> <conn_ID> qsig gf-22

List information pertaining to a specific call-independent connection (as defined by its connection ID)
The response format is as follows:

- NCALL CONN ID : a number in the range of 1-9999 that identifies the call independent connection on a given DSL
- CREF : call reference number in HEX identifying independent connection
- STATE : current state of all call-independent connections (IDLE, CONN_REQ, CONN_EST)
- TIME : year month day hour:minute:second (the time when call independent connection request is made)
- APPL : applications using the call-independent connection (e.g., NACD, NMS,...)
- ORIG : originator
- DEST : destination

To receive information from this response, "GF capability" is required. The QSIG protocols require QsigGF package 305. EuroISDN protocols, for which the CS 1000 supports GF transport, support a smaller set of features, but do not require the QsigGF package.

STAT NWK l	Check status of network card with specified loop, where loop is the even or odd numbered loop on the network card.	basic-1
STAT PER x	Get status of PS card x. x = 0-15, System with Fibre Network Fabric	basic-1
	If the PS card is disabled, the response is changed from DSBL to either: 1. `DSBL` : NOT RESPONDING = PS card x is either missing, faulty or disabled via the faceplate switch. If there is a fault in the extender pair for the network shelf, the status of the PS card will also be: DSBL: NOT RESPONDING. 2. `DSBL` : RESPONDING = The PS card is disabled and responding to the CPU. The PS may have been disabled by manual request (DSPS) or the associated extender pair may have been manually disabled. If neither of these conditions exists, the card may have been disabled because of an overload condition on the associated shelf. Check for OVD messages appearing in previous TTY output. An attempt to enable a PS card which was disabled because of an overload may result in a recurrence of the overload condition: the system's service may be impaired for approximately 2 minutes.	fnf-25
STAT sl	Get current status of superloop and separate carriers on that superloop, based on data previously sent by the Carrier Interface F/W (LCIM). For each carrier, the following fields will be displayed: `S/W State, SPARE Status, NND Status, TSA` (Time Slot Availability) and CALS. `TTSA` = Number of Traffic Timeslots currently available for voice and data calls out of a possible: 21 for T-1 and 27 for T-E. `SPARE Status` indicates whether the carrier is spared and which carrier it is spared in. `NND Status` indicates whether new data calls are disallowed on the timeslots being transmitted by the carrier.	rem_ipe-21
STAT VTRM <cust> <route> <starting member> <number of members>	Displays the status of the virtual trunks for a customer's route starting from a specified starting member for the number of members specified.	basic-4.00

STIF L PDL2 l s c		bri-19
	Displays link status for SAPI 16 interface of BRSC l s c for MPH on loop L.	
STIF L PDL2 L1		bri-19
	Displays the link status for SAPI 16 interface of BRIL L1 for MPH on loop L.	
STIF l PDNI y	Displays the link status for interface Y for PDNI. Where: Loop Y = 1-3	bri-19
STIF l s c DSL DCH x		bri-19
	Displays the link status for B-channel X for the DSL l s c D. Where: BCH stands for B-channel and X = 1–2.	
STAT VTRM <cust #> <route #> <start member> <end member>		basic-3.0
	Display the status of the virtual trunks specified by customer, route, start member and end member numbers.	
STVT <cust #> <route #> <starting member> <number of members>		basic-3.0
	Display the status of the virtual trunks specified by customer, route, start and end member number. **Note:** Not available for CS 1000 Release 4.0 or later.	
SUPL (l)	Print data for all or specified superloop(s).	xpe-15
	loop = 0-252 and must be a superloop (multiples of 4), System with Fibre Network Fabric	fnf-25
TRK l s c u	Seize specified trunk for outpulsing.	basic-1
c u	Small System format Command is valid at a maintenance telephone only. The specified trunk is connected to the maintenance telephone and a test call may be performed on the trunk. When the test call is completed, access sequence SPRE 91 must be redialed to use the maintenance telephone to input more commands.	
XNTT l	Do self-test of Network card for specified superloop. The Network card must be disabled before the self-test.	xpe-15

	loop = 0-252 and must be a superloop (multiples of 4), System with Fibre Network Fabric	fnf-25
XPCT x	Do self-test on Controller x. The NT8D01 Controller must be disabled before the self-test.	xpe-15
XPEC (x)	Print data for all or specified Controller(s).	xpe-15

Chapter 11: LD 33: Peripheral Equipment Diagnostic for Fiber Remote IPE

This module contains commands to perform diagnostic tests of 1.5 Mb/s and fiber remote Intelligent Peripheral Equipment.

Note:
Program 33 is not supported on Small Systems and CS 1000S system.

Fiber Remote IPE diagnostic

The craftsperson may complete any of the following Fiber Remote IPE maintenance operations:

- Enable or disable optical packlets.
- Manually invoke protection switching, at the local or remote side.
- Query status of cards and optical packlets.
- Conduct the loop-back test on the optical receiver-transmitter (EOI) to determine the source of the fault as being the optical fiber span or Fiber remote equipment.
- Run loopback test and continuity tests on optical interface.

Midnight routine operation

Overlay 33 can be scheduled to run at midnight if included in midnight routines. The following actions take place during midnight operation:

- Send Time of Day message to loadware (L/W).
- Print performance monitoring report.
- Run non-service-impacting test on the standby link.
- Run MNSN and MNSP commands to cause protection switching. When these commands are run, continuity tests check both links alternately.

Fibre Network Fabric

The Fibre Network Fabric extends and enhances the 5-group network architecture to 8 non-blocking (inter-group) Network groups, with a resulting expansion in network capacity to 8k timeslots available for Intergroup traffic. This is achieved by using OC-12 SONET rings, and adding additional network and IPE shelves, cards and cables and software changes to allow using the expanded network capacity. This expansion increases the number of available loops from 160 to 256. This applies to Multi Group systems only.

Basic commands for Fiber Remote IPE

AHIN sl	Print all history file (log file) of Fiber superloop sl
AHIP pc	Print all history file of Fiber Peripheral Controller pc
CDSP	Clears the maintenance display on active CPU to 00 or blank
CMIN	Clears minor alarm for all customers
CMIN ALL	Clears minor alarm for all customers
CLPM sl	Clears all performance monitoring counters of Fiber superloop sl (FNET) and its associated FPEC
DSOP sl PRI	Disable optical link of Fiber superloop sl, link Primary
DSOP sl SEC	Disable optical link of Fiber superloop sl, link Secondary
ENOP sl PRI	Enable optical link of Fiber superloop sl, link Primary
ENOP sl SEC	Enable optical link of Fiber superloop sl, link Secondary
FDEF sl	Query default MMI mode on FNET and FPEC of Fiber superloop sl
FNET ALL	Print current status of all Fiber superloops
FNET sl	Print status of Fiber superloop sl (FNET) and its optical packlets
FNTT sl	Test specified Fiber superloop sl (FNET)
FPCT pc	Test specified Fiber peripheral controller pc (FPEC)
FPEC pc	Print status of Fiber peripheral controller pc (FPEC) and its optical packlets

FSTA sl	Print the transmission test status of Fiber superloop sl
FSTP sl	Stop the transmission test. Print test status of Fiber superloop sl
FTST sl test (h/m/s)	Perform a transmission test of Fiber superloop sl for time h/m/s
MNSN sl	Manual switch on Fiber superloop sl (FNET)
MNSP sl	Manual switch on Fiber peripheral controller pc (FPEC)
NHIN sl	Print new history file of Fiber superloop sl (FNET)
NHIP pc	Print new history file of Fiber peripheral controller pc (FPEC)
PRPM sl	Print performance monitoring report for Fiber superloop sl (FNET) and its associated FPEC
SDEF sl LOC	Set default MMI mode on FNET and FPEC of Fiber superloop sl: MMI mode (Local)
SDEF sl REM	Set default MMI mode on FNET and FPEC of Fiber superloop sl: SL-1 mode (Remote)

Alphabetical list of commands

Command	Description	Pack/Rel
AHIN sl	Print all history file (log file) of Fiber superloop sl.	rem_ipe-22
AHIP pc	Print all history file of Fiber Peripheral Controller pc.	rem_ipe-22
CDSP	Clears the maintenance display on active CPU to 00 or blank.	rpe-1
CLPM sl	Clears all performance monitoring counters of Fiber superloop sl (FNET) and its associated FPEC.	rem_ipe-22
CMIN	Clears minor alarm for all customers	alrm_filter-22
CMIN ALL	Clears minor alarm for all customers	rpe-1
DSOP sl PRI	Disable optical link of Fiber superloop sl, link Primary. If that link is active, protection switching occurs. If protection switching is not available, and the FNET is enabled, the command is refused.	rem_ipe-22

Command	Description	Pack/Rel
DSOP sl SEC	Disable optical link of Fiber superloop sl, link Secondary. If that link is active, protection switching occurs. If protection switching is not available, and the FNET is enabled, the command is refused.	rem_ipe-22
ENOP sl PRI	Enable optical link of Fiber superloop sl, link Primary. The command fails if the packet is not physically there.	rem_ipe-22
ENOP sl SEC	Enable optical link of Fiber superloop sl, link Secondary. The command fails if the packlet is not physically there.	rem_ipe-22

FDEF sl	Query default MMI mode on FNET and FPEC of Fiber superloop sl. The system response is:
	`FNET: L/R`
	`FPEC: L/R`
	Where: L = local and R = remote
		rem_ipe-22

FNET ALL	Print current status of all Fiber superloops. The same as FNET sl but repeated for all Fiber superloops in the system.	rem_ipe-22
FNET sl	Print status of Fiber superloop sl (FNET) and its optical packlets. The first line prints the general status of the card and includes: • enable/disable status (known by Software) • PLL status • NNDC (indicates that new data calls are disallowed on this superloop) The next two lines print the status of the packlets: • enable/disable status (known by Firmware) • activity (if selected as active for incoming voice/data) • ALM_LVL - alarm level • ALM_EOI - alarm Electro-Optical Interface (EOI) Presented below is an example of this general Output format, showing possible values. Bold characters indicate fixed titles.	rem_ipe-22

FNET: n	enabled/disabled	locked/ unlocked	NNDC/ <blank>

PACKLETS:	F/W State	Activity	ALM_LVL	ALM_EOI
Primary:	enabled disabled transmission tested	RCV idle	unequipped S.F. S.D. No alarm	Rx Tx Rx Tx No alarm
Secondary:	enabled disabled transmission tested	RCV idle	unequipped S.F. S.D. No alarm	Rx Tx Rx Tx No alarm

Where:

1. unequipped = the optical packlet is physically absent. Firmware treats this as Signal Fail.
2. S.F. = Signal Fail = Out of service. Loadware either switches to the other link or declares "No active link" if Protection Switching (PS) was not possible.
3. S.D. = Signal Degradation = Deteriorated performance. Firmware either switches to the other link, or else the data calls are disallowed if Protection Switching (PS) was not possible. Software handles this state as NNDC.
4. Rx = Receiver alarm
5. Tx = Transmitter alarm

FNTT sl	Test specified Fiber superloop sl (FNET). The Firmware performs a self-test of hardware components and reports results to software. Optical packlets, if present, are also tested. If the FNET is enabled, only the non-active packlet is tested without affecting service. The response may be: `TEST PASSED or TEST FAILED REASON <reason#>`	rem_ipe-22
FPCT pc	Test specified Fiber peripheral controller pc (FPEC). The Firmware performs a self-test of hardware components and reports results to software. Optical packlets, if present, are also tested. If the FPEC is enabled, only the non-active packlet is tested without affecting service. The response may be: `TEST PASSED or TEST FAILED REASON <reason#>`	rem_ipe-22
FPEC pc	Print status of Fiber peripheral controller pc (FPEC) and its optical packlets. The first line prints the general status of the card. The next two lines print the status	rem_ipe-22

	of the packlets. See FNET description for more detail.	
FSTA sl	Print the transmission test status of Fiber superloop sl.	rem_ipe-22
FSTP sl	Stop the transmission test. Print test status of Fiber superloop sl.	rem_ipe-22
FTST sl test (h/m/s)		rem_ipe-22
	Perform specified transmission test of Fiber superloop sl for time tm. Where: • test = 1 for FNET primary packlet ; 2 for FPEC primary packlet ; 3 for FNET secondary packlet ; 4 for FPEC secondary packlet • tm = H/M/S = test duration. This field is optional. The duration can be either: - H for hours (1-24) - M for minutes (1-255) - S for seconds (1-255) If a duration is not entered, then Firmware performs a quick test and reports the results to software. The system response will then be `TEST SUCCESS or TEST FAILED .` If duration is entered, then firmware starts testing and sends an acknowledge message to software. The system response will be `TEST STARTED .` These transmission tests can only be executed on the standby or disabled link.	
MNSN sl	Manual switch on Fiber superloop sl (FNET). The FNET loadware switches between the active link and the standby link.	rem_ipe-22
MNSP pc	Manual switch on Fiber peripheral controller pc (FPEC). The FPEC loadware switches between the active link and the standby link.	rem_ipe-22
NHIN sl	Print new history file of Fiber superloop sl (FNET)	rem_ipe-22
NHIP pc	Print new history file of Fiber peripheral controller pc (FPEC)	rem_ipe-22
PRPM sl	Print performance monitoring report for Fiber superloop sl (FNET) and its associated FPEC.	rem_ipe-22

SDEF sl LOC	Set default MMI mode on FNET and FPEC of Fiber superloop sl : MMI mode (Local)	rem_ipe-22
SDEF sl REM	Set default MMI mode on FNET and FPEC of Fiber superloop sl : SL-1 mode (Remote)	rem_ipe-22

Chapter 12: LD 34: Tone and Digit Switch and Digitone Receiver Diagnostic

This program tests circuit cards used in generating and detecting tones in the Meridian 1/Meridian SL-1 system. If loaded automatically in background or as part of the daily routines, it tests the hardware and performs fault detection and isolation. If invoked manually, commands can be issued to conduct the entire test or only certain parts of the test and to change card status.

The program tests the following circuit cards:

- Tone and Digit Switch (TDS)
- Flexible Tone and Digit Switch
- Digitone Receiver (DTR)
- Tone Detector
- Dial Tone Detector
- Extended Tone Detector (XTD)

TDS circuit card outpulsers and channels are checked for timing errors, memory faults and Digitone frequency accuracy. Digitone receivers are checked for response to all Digitone frequencies. Tones and outpulses are tested from a maintenance set.

Fibre Network Fabric

The Fibre Network Fabric extends and enhances the 5-group network architecture to 8 non-blocking (inter-group) Network groups, with a resulting expansion in network capacity to 8k timeslots available for Intergroup traffic. This is achieved by using OC-12 SONET rings, and adding additional network and IPE shelves, cards and cables and software changes to allow using the expanded network capacity. This expansion increases the number of available loops from 160 to 256. This applies to Multi Group systems only.

Basic commands

Contents

Section
Large System and Avaya Communication Server 1000E System commands on page 144
Small Systems, CS 1000S, MG 1000B, and MG 1000T commands
Extended Tone Detector (XTD) commands on page 145
Maintenance telephone commands on page 146

Large System and Avaya Communication Server 1000E System commands

The following commands are applicable to all Large System and Avaya CS 1000E Systems.

CDSP	Clear the maintenance display on active CPU to 00 or blank
CMAJ	Clear major alarm and reset power fail transfer
CMIN	Clears minor alarm for all customers
CMIN ALL	Clears minor alarm for all customers
DISD l s c	Disable the specified Meridian 1/Meridian SL-1 Tone Detector card
DISD l s c u	Disable specified Dial Tone Detector
DISL loop	Disable tone and digit loop
DISR l s c (u)	Disable specified DTR/MFR card or unit. Applies to DTR or XTD cards.
DISM (sulp) s	Disable configured Media Gateway TDS loops on IPMG
DISX l	Disable Conf/TDS/MFS card on loop l and l + 1
DTD l s c u	Test specified Dial Tone Detector unit. Applies to DTD and XTD cards.

DTR l s c (u)	Test specified Digitone receiver card or unit. Applies to DTR and XTD cards.
END	Stop execution of current command
ENLD l s c (u)	Enable Tone Detector on specified card or unit
ENLL loop	Enable tone and digit loop
ENLR l s c (u)	Enable the DTR/MFR card or unit. Applies to DTR and XTD cards.
ENLM (sulp) s	Enable configured Media Gateway TDS loops on IPMG
ENLX l	Enable Conf/TDS/MFS card on loop l and l + 1
MFR	Test all Automatic Number Identification Feature Group D Multifrequency receiver units
MFR loop	Test all Automatic Number Identification Feature Group D Multifrequency receiver units on specified loop
MFR l s c (u)	Test Automatic Number Identification Feature Group D Multifrequency card or unit
SDTR l s c (u)	Get status of specified DTR/MFR or XTD card or unit.
STAD	List all disabled Tone Detector units
STAD l s c (u)	Get status of Tone Detector card or unit
STAT	List TNs of all disabled DTRs and MFRs
STAT loop	Get status TDS loop
TDET l s c (u)	Perform self-test and tone detection on specified card or unit
TDS loop	Test outpulsers and channels on specified loop

Extended Tone Detector (XTD) commands

The following commands are applicable to the NT5K20 and NT5K48 XTD cards:

DISR l s c (u)	Disable the specified XTD card (or unit)
DTR l s c u	Test the specified XTD unit as a Digitone receiver unit
ENLR l s c (u)	Enable the specified XTD card (or unit)
SDTR	List Terminal Numbers (TN) of all disabled DTR units
SDTR l s c (u)	List the status of the specified XTD card (or unit)

Maintenance telephone commands

The following commands are used from a Maintenance telephone to test and hear the various tones. Both the command and the dial pad equivalents (in parantheses) are shown.

ANNx#loop## (266x#loop##)		basic-6
	Provides signals coming through source number x of KAPSCH Digital Announcer or Music Interface. Where loop = Tone and Digit Switch loop number)	
BSY#loop## (279#loop##)		basic-1
	Provide busy tone from tone and digit loop.	
C## (2##)	Remove any active tone.	basic-1
CMP#loop## (267#loop##)		basic-1
	Provide Camp-On tone from loop.	
CUST#xx## (2878#xx##)		basic-1
	Test outpulsing for customer XX.	
CWG#loop## (294#loop##)		basic-1
	Give call waiting tone from loop.	
DIA#loop## (342#loop##)		basic-1
	Provide dial tone from tone and digit loop.	
DRNG#loop## (3764#loop##)		basic-1
	Provide distinctive ringing from loop.	
ITN#loop## (486#loop##)		basic-1
	Provide intrusion tone from loop.	
JDRG#loop## (5374#loop##)		basic-8
	Provide distinctive ringing from loop.	
JIDT#loop## (5438#loop##)		basic-8
	Provide interrupted dial tone from loop.	
OPS#loop#x## (677#loop#x##)		basic-1
	Test outpulsing from Meridian 1/Meridian SL-1 to idle trunk.	
ORD#loop## (673#loop##)		basic-1
	Provide override tone from loop.	

OVF#loop## (683#loop##) basic-1

Provide overflow tone from loop.

PCRT#loop## (7278#loop##) pcr-7

Test the Paid Call Restriction (PCR) tone after the TABL command.

RBK#loop## (725#loop##) basic-1

Provide ringback tone from loop.

RNG#loop## (764#loop##) basic-1

Provide ring tone from loop.

SDL#loop## (735#loop##) basic-1

Give special dial tone from loop.

TABL#xx## (8225#xx##) basic-1

Select table number xx. If this command is not issued before any tone request command, then table 0 is assumed (Generic software with supplementary features).

TLP#loop## (857#loop##) basic-4

Provide tone to last party from the tone and digit loop.

TST#loop## (878#loop##) basic-1

Provide test tone from loop.

XCTT#loop#t#c## (9288#loop#t#c##) xct-15

Test tone and cadence number on Conference/TDS/MFS card.

Alphabetical list of commands

Command	Description	Pack/Rel
ANNx#loop## (266x#loop##)		basic-6
	Provides signals coming through source number x of KAPSCH Digital Announcer or Music Interface. Where:loop = Tone and Digit Switch loop number.	
BSY#L## (279#L##)		
	Provide busy tone from tone and digit loop L.	basic-1

Command	Description	Pack/Rel
C## (2##)	Remove any active tone.	basic-1
CDSP	Clear the maintenance display on active CPU to 00 or blank.	basic-1
CMAJ	Clear major alarm, reset power fail transfer and clear power fault alarm.	basic-1
CMIN	Clears minor alarm for all customers	alrm_filter-22
CMIN ALL	Clears minor alarm for all customers	basic-1
CMP#loop## (267#loop##)	Provide Camp-On tone from loop.	basic-1
CUST#xx## (2878#xx##)	Test outpulsing for customer XX.	basic-1
CWG#loop## (294#loop##)	Give call waiting tone from loop.	basic-1
DIA#L## (342#L##)	Provide dial tone from tone and digit loop L.	basic-1
DISD l s c	Disable the specified Tone Detector card. Disables both units and lights the LED.	basic-1
DISD l s c u	Disable specified Dial Tone Detector. If both units on the card are disabled, the LED lights.	basic-1
DISL loop	Disable tone and digit loop. For Conference/TDS/MFS cards see note with ENLL command.	basic-1
DISM (sulp) s	Disable configured Media Gateway TDS loops on IPMG.	ipmg-5.00
DISR l s c (u)	Disable specified DTR/MFR or XTD card or unit.	xtd-8
DISX l	Disable Conf/TDS/MFS card on loop l and l + 1. Disables the entire combined Conference, Tone and Digit Switch, and MF Sender (NT8D17) card. Both the even numbered TDS/MFS loop and adjacent conference loop are disabled. loop = 0, 2, 4,. . . 254	xct-15

Command	Description	Pack/Rel
	]The DISL and ENLL commands can be used on the even number loop for the TDS/MFS functions. However, this only prevents the loop from being used by software and does not affect the hardware status of the card. The DISX and ENLX commands are recommended. The ENLX command must be used if the DISX command was used to disable the card. This command can be used in LD 34, LD 38 and LD 46.	
DRNG#loop## (3764#loop##)		basic-1
	Provide distinctive ringing from loop.	
DTD l s c u	Test specified Dial Tone Detector unit. Applies to DTD and XTD cards. The Dial Tone Detector Test (DTDT) parameters must be configured in the configuration record (LD 17). Faulty DTD cards are disabled. Only 50% of all Dial Tone Detectors in the system may be disabled.	xtd-8
DTR l s c (u)	Test specified unit on Digitone receiver card or unit. This test may be performed while the card is enabled or disabled. If a disabled card passes the test, it is enabled automatically. This command also applies to the XTD.	xtd-8
END	Stop execution of current command.	basic-1
ENLD l s c (u)	Enable Tone Detector on specified card or unit.	basic-1
ENLL l	Enable tone and digit switch loop l. For Conference/TDS/MFS cards the DISX and ENLX commands must be used whenever the faceplate switch of the card has been toggled. ENLL will software enable the card but the card will not be properly reset.	basic-1
ENLM (sulp) s	Enable configured Media Gateway TDS loops on IPMG.	ipmg-5.00
ENLR c (u)	Enable the DTR/MFR or XTD card or specified unit. This command applies to any units on card 0 regardless of its configured type.	xtd-8
ENLR l s c (u)	Enable the DTR/MFR or XTD card or specified unit.	xtd-8
ENLX c	Enable the TDS/MFS card This command enables TDS and alll units on card 0. For Card 0, this command initiates the card reset sequence: it downloads any parameters required for any configured MFC/MFE/MFK5/MFK6 units.	basic-22

Command	Description	Pack/Rel
ENLX l	Enable Conf/TDS/MFS card on loop l and l + 1. This command can be used in LD 34, LD 38 and LD 46. Enables the entire combined Conference, Tone and Digit Switch, and MF Sender (NT8D17) card. Both the even numbered TDS/MFS loop and adjacent conference loop are enabled. (loop = 0, 2, 4,. . . 254) The Conf/TDS card is not enabled automatically when it is inserted. Both loops must have been previously disabled. This command initiates card tests and the download of software. The DISL and ENLL commands can be used on the even number loop for the TDS/MFS functions. However, this only prevents the loop from being used by software and does not affect the hardware status of the card. The DISX and ENLX commands are recommended. The ENLX command must be used if the DISX command was used to disable the card. Enabling more than 16 conference loops may cause the system to lock-up.	xct-15
ITN#loop## (486#loop##)	Provide intrusion tone from loop.	basic-1
JDRG#loop## (5374#loop##)	Provide distinctive ringing from loop.	basic-8
JIDT#loop## (5438#loop##)	Provide interrupted dial tone from loop.	basic-8
MFR	Test all Automatic Number Identification (ANI) Multifrequency receiver units.	fgd-17
MFR loop	Test all Automatic Number Identification (ANI) Multifrequency receivers on this loop.	fgd-17
MFR l s c (u)	Test Automatic Number Identification (ANI) Multifrequency receiver card or unit.	fgd-17
OPS#L#xx## (677 #L #xx##)	Test outpulsing from Meridian 1/Meridian SL-1 to idle trunk. Outpulses from tone and digit loop l using the 10 or 20 pps outpulser to any idle trunk. This command connects the maintenance telephone to the trunk, permitting a test call	basic-1

Command	Description	Pack/Rel
	on the trunk to be made using the outpulsers selected, where: xx = 10 or 20 representing the trunk class of service (LD 14 CLS = P10 or P20). When the test call is completed, LD 34 must be reloaded by dialing SPRE + 91 before entering another command.	
ORD#loop## (673#loop##)		basic-1
	Provide override tone from loop.	
OVF#L## (683#L##)		
	Provide overflow tone from loop L.	basic-1
PCRT#loop## (7278#loop##)		pcr-7
	Test the Paid Call Restriction (PCR) tone after the TABL command.	
RBK#L## (725#L##)		
	Provide ringback tone from loop L.	basic-1
RNG#L## (764#L##)		
	Provide ring tone from loop L.	basic-1
SDL#loop## (735#loop##)		basic-1
	Give special dial tone from loop.	
SDTR	List the TNs of all disabled DTR/MFR or XTD units	xtd-8
SDTR	List all disabled DTR units	basic-1
SDTR l s c (u)	Get status of specified DTR/MFR or XTD card or unit. If no parameters are entered, a list of all DTR/MFR TNs is output. If l s c is input, the status of the DTR/MFR units on the specified card are output. If l s c u is input, the status of the specified unit is output. Applies to DTR and XTD cards.	basic-1
STAD	List all disabled Tone Detector units.	basic-1
STAD l s c (u)		

Command	Description	Pack/Rel
	Get status of Tone Detector card or unit. The status is either idle, busy, maintenance busy or not equipped.	basic-1
STAT	List TNs of all disabled Digitone Receivers. NONE is output if there are no disabled Digitone Receivers.	basic-1
STAT c	Show TDS status and number of disabled or busy tone transmitter channels. The STAT c command is used for the SSTD or CPU card.	basic-1
STAT loop	Get status TDS loop. The response may include OPS DSBL, indicating that the outpulsing function of the TDS card has been disabled.	basic-1
TABL#xx## (8225#xx##)		basic-1
	Select table number xx. If this command is not issued before any tone request command, then table 0 is assumed. (Generic software with supplementary features).	
TDET l s c (u)		
	Perform self-test and tone detection on specified card or unit. Performs the self-test and basic tone detection functions of the Meridian 1/Meridian SL-1 Tone Detector card or unit. This test may be performed while the card is enabled or disabled. If a disabled card passes the test, it is enabled automatically.	basic-1
TDS loop	Test outpulsers and channels on specified loop. Tests the outpulsers and channels of the tone and digit switch at loop. Outpulsers and tones are tested with a maintenance telephone (see commands from maintenance telephone).	basic-1
TDS card	Test outpulsers and channels on specified card. When the Fast Tone and Digit Switch (FTDS) package 87 is equipped, it: • tests the outpulsers and channels of the tone and digit switch • outpulses 32 digits to a DTR, receives and stores the 32 digits from the DTR	basic-1

Command	Description	Pack/Rel
	• tests that the time to outpulse 32 digits is within an acceptable range • compares the outpulsed 32 digits with those received and displays OK if they match	
TLP#loop## (857#loop##)	Provide tone to last party from the tone and digit loop.	basic-4
TST#loop## (878#loop##)	Provide test tone from loop.	basic-1
XCTT# L#t#c## (9288# L#t#c##)	Test tone and cadence number on Conference/TDS/MFS card, where: • L = loop number of Conference/TDS/MFS (NT8D17) card • t = tone number • c = cadence number Refer to Flexible Tone and Digit Switch cards (553-2711-180) for the Conference/TDS tone and cadence numbers.	xct-15

Chapter 13: LD 36: Trunk Diagnostic

This program allow trunks to be tested from either the system site or a remote test center.

When testing from a system, individual trunks can be seized and a test call can be performed on the trunk in the normal manner.

When testing from a remote test center, a speech path must be set up to monitor the testing. This is accomplished by having the system call a directory number (DN) at the test center. This allows for dial tone, outpulsing and test tones to be monitored as tests are performed on other trunks by inputting commands at the TTY.

When a trunk is seized, the system prompts DN? for a DN. When the DN is input, the system calls that number automatically. When the call is answered a pure tone indicates the validity of the speech path. New trunks can be tested in the same manner with the maintenance telephone.

Note:
When the French (FRTA) package 197 is enabled the units on CO trunks are not busied when they are disabled.

Note:
When the Trunk Failure Monitor (TFM) package 182 is enabled, a failed trunk is displayed as BUSY. The enable/disable command does not enable or disable the failed trunk unit (it stays in the BUSY state).

When to use LD 36

Use LD 36 to:

- clear minor alarms and the maintenance display
- query threshold overflows for specific customers and routes
- reset thresholds for specific trunks
- query number of days since an incoming call was received for a specific customer and route or trunk
- query the trunk with the most number of idle days for a specific customer and route
- query trunks for which no disconnect supervision was received
- test Automatic Number Identification (ANI) trunks.

Note:
When defined as a midnight routine, this program searches for trunks not used during the day and updates the total number of days the trunks have been idle.

Note:
LD 36 can only be used for analog trunks, LD 60 must be used for diagnostics on digital trunks.

Trunk error thresholds

Resident programs monitor all calls and note apparent errors. The errors are accumulated and, if they occur consistently (exceed a threshold) on any trunk, a diagnostic message which identifies the trunk is output to the TTY or printer. The trunk should be suspected of trouble and a manual test should be performed on the trunk.

A record is kept in memory for each threshold violation error message. At any time, all trunks which have been identified by such a message may be listed by entering the command LOVF for any trunk route. Once an identifying message has been printed, it will not be repeated for that trunk until the RSET command is entered for that trunk or an initialization has occurred.

Potentially, a trunk may fail by not detecting incoming calls. The Meridian 1/Meridian SL-1 threshold mechanism cannot be used to detect such failures so the Meridian 1/Meridian SL-1 maintains for each trunk a count of the number of days since an incoming call was received on each trunk.

Thus, customer reports that indicate incoming calls are not being processed can initiate a check for the trunk which has been without an incoming call for the longest interval via the LMAX command. This trunk should be tested first.

It is possible to determine for each trunk the number of days since an incoming call was processed via the LDIC command. Subsequent trunk tests should be performed on those trunks showing the highest counts until the trouble is located.

Fibre Network Fabric

The Fibre Network Fabric extends and enhances the 5-group network architecture to 8 non-blocking (inter-group) Network groups, with a resulting expansion in network capacity to 8k timeslots available for Intergroup traffic. This is achieved by using OC-12 SONET rings, and adding additional network and IPE shelves, cards and cables and software changes to allow using the expanded network capacity. This expansion increases the number of available loops from 160 to 256. This applies to Multi Group systems only.

Basic commands (LD 36)

The following commands are applicable to all Large System and CS 1000E Systems.

CALL	Set up monitor link with test center
CALL l s c u	Set monitor link with test center on this trunk
CDSP	Clear the maintenance display on active CPU to 00 or blank
CMIN	Clears minor alarm for all customers
CMIN ALL	Clears minor alarm for all customers
DISC l s c	Disable specified card for replacement
DISU l s c u	Disable specified unit
END	Terminate test in progress
ENLC l s c	Enable specified card
ENLU l s c u	Enable specified unit
LDIC c r	List number of days since last incoming call for specified customer and route
LDIC l s c u	List number of days since last incoming call on specified trunk
LMAX c r	List trunk with maximum idle days for specified customer and route
LNDS c r	List trunks with no disconnect supervision for specified customer and route
LOVF c r	List threshold overflows for specified customer and route
RAN c r	Test recorded announcement device for specified customer and route
RLS	Release trunk being tested
RSET l s c u	Reset thresholds for specified trunk
STAT l s c	Check card's software status
TRK l s c u	Seize trunk for testing
TPPM l s c u	Test the specified PPM trunk

Note:
If a trunk unit is controlled by APNSS, the STAT command will display the status of the D-channel.

Alphabetical list of commands

Command	Description	Pack/Rel
CALL	Set up monitor link with test center. Same as the CALL l s c command except any PTRS trunk in the system can be selected. The CALL command must be terminated using the * command.	basic-1
CALL l s c u	This command sets up a monitor link (call) between the system and the test center on the trunk specified. The system prompts "DN?" for the directory number. When the PTRS directory number is entered, the system calls up that number automatically. When the call is answered, a pure tone indicates the validity of the link. This sequence can take up to 14 seconds on a trunk without answer supervision. The END command disconnects the call. The CALL l s c u command is not allowed when the diagnostic program is being run from a maintenance telephone. During the CALL command, On-Hook and Off-Hook signals from the maintenance telephone may initiate BUG105. When the monitor is enabled, a failed trunk is displayed as BUSY. The enable/disable command does not enable or disable the failed trunk unit (it stays in the BUSY state).	basic-1
CDSP	Clear the maintenance display on active CPU to 00 or blank.	basic-1
CMIN	Clears minor alarm for all customers	alrm_filter-22
CMIN ALL	Clears minor alarm for all customers	basic-1
DISC l s c	Disable specified card for replacement.	basic-1
DISU l s c u	Disable specified unit.	basic-1
END	Terminate test in progress	basic-1
ENLC l s c	Enable specified card. If the card resides on a disabled shelf, its status is output and the enable is not performed. If the card has	basic-1

Command	Description	Pack/Rel
	been disabled by an overload, the overload status is cleared.	
ENLU l s c u	Enable specified unit. If unit resides on a disabled shelf or card, then status is output and enable is not performed.	basic-1
LDIC c r	List number of days since last incoming call for specified customer (c) and route (r).	basic-1
LDIC l s c u	List number of days since last incoming call on specified trunk.	basic-1
LMAX c r	List trunk with maximum idle days for specified customer and route	basic-1
LNDS c r	List trunks with no disconnect supervision for specified customer and route. (trunks for which no disconnect supervision was received, i.e., terminating party not going On-Hook after a call)	basic-1
LOVF c r	List threshold overflows for specified customer and route. The overflows are set when the resident trunk monitor outputs a diagnostic	basic-1
RAN c r	Test recorded announcement device for specified customer and route.	basic-1
RLS	Release trunk being tested.	
RSET l s c u	Reset thresholds for specified trunk.	basic-1
STAT l s c	Check card's software status.	basic-1
STAT tn	Check analog trunk card's software status	x21-basic-2
TPPM l s c u	Test the specified PPM trunk. This command is not applicable when the system is connected to 1 TR 6 international ISDN PRA.	basic-1
TRK l s c u	Seize trunk for testing. Seizes the specified trunk for outpulsing and testing. If the command is issued from a maintenance telephone, dial tone is heard followed by outpulsing when the directory number is entered. If a trunk is to be seized for outpulsing and testing from a remote test center (not a maintenance telephone), a	basic-1

Command	Description	Pack/Rel
	monitor link must first be set up using the CALL l s c u command. This must not be over the trunk to be tested. With the monitor link set up, the TRK l s c u command is input to select the trunk to be tested. The system then prompts with "DN?" and the directory number is input via the TTY. Normal speech path connections are made between the monitor link and the trunk being tested. Disconnect by entering END, by going On-Hook if an SL-1 telephone is used or by entering *. END also disconnects the monitor link. This command cannot be used to seize an ISL trunk.	

Chapter 14: Input/Output Diagnostic

This program is used to diagnose faults with disk units, Teletypewriter (TTY) or Serial Data Interface (SDI) cards. It provides enable, disable, status and test functions on these devices. Problems are indicated in IOD messages.

When LD 37 is defined as a daily routine, the program runs only once every 5 days and the primary storage device is thoroughly tested.

Only some of the commands in this Overlay are supported by Options 51C, 61C, and 81C. Refer to LD 137 for core commands.

Refer to LD 48 for I/O ports used with the following applications:

- Command and Status Links (CSL)
- Meridian Link
- Automatic Call Distribution (ACD)
- Integrated System Messaging Link
- Enhanced Serial Data Interface (ESDI) ports

Intelligent links (APL, HSL, and LSL)

A warning message is generated each time an intelligent link is accessed (enable, disable, test). The message is generated for the following types of links:

- APL
- ACD-D (HSL/LSL)

The message allows the access to be aborted prior to performing the enable, test, etc. The warning appears in the following format:

DIS TTY N (link type) LINK (status) (y/n)

A response of y disables the hardware of the TTY regardless of the software status of the link. The status field provides the software status of the link. Valid status entries are:

BAD = software status is invalid DOWN = link is down MAINT = link is up and in maintenance mode FULL = link is full EMPTY = link is empty NOT EMPTY= link still contains data

If LD 37 is run as part of the daily routines, an IOD075 message will be output on systems equipped with disk drives. This message should be disregarded.

D-channel Expansion

With the introduction of D-channel Expansion, new software allows the increase of D-channels past sixty-four. Instead of the Large System having a maximum of 16 I/O addresses, the new software allows 16 physical I/O addresses (0 - 15) per network group for D-channels defined on MSDL. With this enhancement a response to the system response GROUP is required to inform the system of the desired network group.

Note:
See "D-channel Expansion commands" in LD-48 or LD-96 for a complete description of these commands.

Basic commands

CDSP	Clear the maintenance display on active CPU to 00 or blank
CMIN	Clears minor alarm for all customers
CMIN ALL	Clears minor alarm for all customers
DIS MSG	Disable incoming message monitoring for the primary PMSI port.
DIS MSGO	Disable outgoing message monitoring for the primary PMSI port.
DIS MSI x	Disable Mass Storage Interface card x (not valid on Small System)
DIS PRT x	Disable printer x
DIS TTY x	Disable TTY x. (valid only for Card 0 Port 0 TTY on Small Systems and CS 1000S systems)
END	Clear all test activity
ENL MSGI	Enable incoming message monitoring for the primary PMSI port.
ENL MSGO	Enable outgoing message monitoring for the primary PMSI port.
ENL MSI x	Enable Mass Storage Interface x
ENL PRT x	Enable printer x
ENL TTY x	Enable TTY x
MSI x	Test Mass Storage unit x (not valid on Small System)

MSI DATA	Test data validity in primary and backup device. (not valid on Small System)
MSI RW x	Test READ/WRITE ability of Mass Storage unit x. (not valid on Small System)
MSI SELF x	Perform self-test on MSI card x and report result. (not valid on Small System)
PRT x	Test printer x
SET MON 0	Set the monitoring display to be in alphanumeric format. This applies to the primary PMSI port.
SET MON 1	Set the monitoring display to be in hexadecimal format. This applies to the primary PMSI port.
STAT	Provide status of all input/output devices in system
STAT LINK	Provide status of all CDR links
STAT LINK x	Provide status of CDR data link x
STAT MON	Get the monitoring status for the primary PMSI port. This command displays the status of the message monitoring for the primary port. For example, if MSGI, MSGO, and SET MON 0 are enabled, the display would be as follows. MSGI:ON MSGO: ON ALPH
STAT MSI	Provide status of all MSI cards
STAT MSI x	Provide status of MSI card x
STAT PRT	Provide status of all printers in system
STAT PRT x	Provide status of printer x
STAT TTY	Provide status of all TTY devices in system This command enables you to get the status of the primary PMSI I/O port, and the Single Terminal Access (STA) administration terminal.
STAT TTY x	Provide status of TTY x This command also provides the status of the primary PMSI port.
STAT XSM	Provide status of the system monitor
TTY x	Test TTY x

Multipurpose Serial Data Link (MSDL) commands

The MSDL provides 4 ports for ISDN Primary Rate D-channel (DCH) and Application Module Link (AML).

The MSDL commands are listed below, x is the MSDL device number (defined by prompt DNUM in LD 17). These commands are provided in Link Diagnostic (LD 48) and D-channel Diagnostic (LD 96).

DIS MSDL x (ALL)	Disable MSDL device x (card)
ENL MSDL x (ALL, FDL)	Enable MSDL device x (card, Forced Download)
RST MSDL x	Reset MSDL device x
SLFT MSDL x	Invoke self-test for MSDL device x
STAT MSDL (x) (FULL)	Get status of MSDL card (x) (additional information)

Note:
See "Alphabetical List of commands" in LD 48 for a complete description of these commands.

Alphabetical list of commands

Command	Description	Pack/Rel
CDSP	Clear the maintenance display on active CPU to 00 or blank.	basic-1
CMIN	Clears minor alarm for all customers	alrm_filter-22
CMIN ALL	Clears minor alarm for all customers	basic-1
DIS MSG	Disable incoming message monitoring for the primary PMSI port.	pms-19
DIS MSGO	Disable outgoing message monitoring for the primary PMSI port.	pms-19
DIS MSDL x (ALL)	Disable MSDL device x	

Command	Description	Pack/Rel
DIS PRT x	Disable printer x.	basic-1
DIS TTY x	Disable TTY x. Only valid for Card 0 Port 0 TTY on Small Systems and CS 1000S systems.	basic-1
END	Clear all test activity.	basic-1
ENL MSGI	Enable incoming message monitoring for the primary PMSI port.	pms-19
ENL MSGO	Enable outgoing message monitoring for the primary PMSI port.	pms-19
ENL MSDL x (ALL, FDL)		
	Enable MSDL device x	
ENL PRT x	Enable printer x.	basic-1
ENL TTY x	Enable TTY x.	basic-1
PRT x	Test printer x. Same as TTY test except that no keyboard input is expected and END command is not required. Where: * denotes that the printer is not yet available	basic-1
RST MSDL x	Reset MSDL device x	
SET MON 0	Set the monitoring display to be in alphanumeric format. This applies to the primary PMSI port.	pms-19
SET MON 1	Set the monitoring display to be in hexadecimal format. This applies to the primary PMSI port.	pms-19
SLFT MSDL x	Invoke self-test for MSDL device x	
STAT	Provide status of all input/output devices in system.	basic-1
STAT MON	Get the monitoring status for the primary PMSI port. This command displays the status of the message monitoring for the primary port. For example, if MSGI, MSGO, and SET MON 0 are enabled, the display would be as follows. `MSGI:ON MSGO: ON ALPH`	pms-19
STAT MSDL (x [FULL])		
	Get MSDL status	
STAT PRT	Provide status of all printers in system.	basic-1
STAT PRT x	Provide status of printer x.	basic-1
STAT TTY	Provide status of all TTY devices in system. This command enables you to get the status of the primary PMSI I/O port, and the Single Terminal Access (STA) administration terminal.	basic-1

Command	Description	Pack/Rel
STAT TTY x	Provide status of TTY x. This command also provides the status of the primary PMSI port.	basic-1
STAT XSM	Provide status of the system monitor. If there are no error conditions, PWR000 is output. Otherwise, the appropriate PWR messages are output.	xpe-15

TTY x	Test TTY x. Response is:
	`ABCDEFGHIJKLMNOPQRSTUVWXYZ`
	`0123456789"#$%*!&()<>—.:,.? READY FOR INPUT`
	Anything entered on the keyboard will be echoed until END is input.
		basic-1

Chapter 15: LD 38: Conference Circuit Diagnostic

This program is used to detect and isolate circuit faults on the conference equipment in the system.

LD 38 can detect problems on the conference circuit such as:

- channel faults on the network card which interfaces a conference card to the system
- channel faults on the conference card or IP-based conference loop
- conference faults associated with conferee group numbers
- switching faults controlling the attenuation feature.

The program is used to:

- enable a specific conference card or IP-based conference loop
- disable a specific conference card or IP-based conference loop
- check status of channels and conferee groups
- clear alarms and displays

The program allows complete manual control in establishing a test conference, thus allowing the user to listen for noise and distortion. This includes:

- selection of a specific conference card or IP-based conference loop
- selection of a specific conferee group
- stepping through all free channels and groups with special test conference.

Some commands are not valid on Small Systems and CS 1000S, since the conference circuits are always enabled.

Note:
Loops 29 and 30 are on the CPU/CONF card and loop 31 is on the Expansion Cabinet Data Cartridge (for Small System only).

Fibre Network Fabric

The Fibre Network Fabric extends and enhances the 5-group network architecture to 8 non-blocking (inter-group) Network groups, with a resulting expansion in network capacity to 8k timeslots available for Intergroup traffic. This is achieved by using OC-12 SONET rings, and adding additional network and IPE shelves, cards and cables and software changes to allow

using the expanded network capacity. This expansion increases the number of available loops from 160 to 256. This applies to Multi Group systems only.

Basic commands

CDSP	Clears the maintenance display on active CPU to 00 or blank
CMIN	Clears minor alarm for all customers
CMIN ALL	Clears minor alarm for all customers
CNFC loop	Test conference loop
CNFC MAN loop g	Set up for manual conference on conference group g
CNFC STEP	Ready TTY for testing conferee groups
DISL loop	Disable conference loop
DISX loop	Disable Conf/TDS/MFS card on loop and loop - 1 (Large Systems)
END	Abort all current test activity
ENLL loop	Enable conference loop
ENLX loop	Enable Conf/TDS/MFS card on loop and loop - 1 (Large Systems)
LCNF loop	List busy and disabled conferee groups on specified loop
STAT loop	Provide status of conference card or IP-based conference loop
STAT c u	List conference card and group used by specified TN. (Small System)
STAT l s c u	List conference card or IP-based conference loop and group used by specified TN.

Alphabetical list of commands

Command	Description	Pack/Rel
CDSP	Clears the maintenance display on active CPU to 00 or blank.	basic-1

Command	Description	Pack/Rel
CMIN	Clears minor alarm for all customers	alrm_filter-22
CMIN ALL	Clears minor alarm for all customers	basic-1
CNFC loop	Test conference loop. Tests conference loop for channel, group and switching faults. **Note:** Both the conference loop and the adjacent TDS/ MFS loop must be enabled to run the conference test.	basic-1
CNFC MAN loop g	Set up for manual conference on conference group g. Only one manual conference is be allowed at a time. The conference group range is 1-15. After this command, any telephone dialing SPRE 93 enters the conference, where SPRE is the special service prefix for the system. Going on-hook from that telephone takes it out of the conference. If going On-Hook causes the conference to go from a three-party to a two-party call processing may remove all conference equipment and establish the remaining two parties as a normal call. The END command, which normally removes all telephones in the manual conference, will no longer affect these two telephones, as they are no longer using the conference card. If the CNFC MAN command is entered from a maintenance set, the telephone automatically becomes part of the manual conference.	basic-1
CNFC STEP	Ready TTY for testing conferee groups. Readies the TTY into a special command mode for testing various channels and conferee groups audibly, using two telephones: one to monitor and one to act as a signal source. The CNFC MAN command should have been used previously to set up the two-party conference. Entering C on the command input device will step the conference on to the next available channel. Entering G will step to the next available conferee group. Entering an asterisk (*) will revert back to the normal command mode. Entering "END" or aborting LD 38 releases the manual conference.	basic-1

Command	Description	Pack/Rel
DISL loop	Disable conference loop. For NT8D17 Conference/TDS/MFS cards, see ENLL command. **Note:** Disabling an IP conference loop on the Call Server does not change its registration status on the Media Services Controller (MSC). The disabled conference loop is not listed as a conference resource on the Call Server but it still appears in the RLM table on the MSC. You must remove the loop using LD 17 to delete its RLM table entry from the MSC.	basic-1
DISX loop	Disable NT8D17 Conf/TDS/MFS card. Disables the entire combined Conference, Tone and Digit Switch, and MF Sender (XCT) card. Both the even numbered and adjacent loop are disabled, where: loop = 1, 3, 5,... 255, System with Fibre Network Fabric The DISL and ENLL commands can be used on the even number loop for the conference function. However, this only prevents the loop from being used by software and does not affect the hardware status of the card. The DISX and ENLX commands are recommended. The ENLX command must be used if the DISX command was used to disable the card. This command can be used in LD 34, LD 38 and LD 46.	xct-15 fnf-25
END	Abort all current test activity. There will be a 30 second time-out dial tone for phones still off-hook.	basic-1
ENLL loop	Enable conference loop. For NT8D17 Conference/TDS/MFS cards the DISX and ENLX commands must be used whenever the faceplate switch of the card has been toggled. ENLL will software enable the card but the card will not be properly reset. Enabling more than 16 conference loops may cause system to lock-up. **Note:** Enabling or disabling an IP conference loop on the Call Server does not change its registration status on the Media Services Controller (MSC). The RLM table entry for the loop on the MSC is not impacted by the ENLL command.	basic-1

Command	Description	Pack/Rel
ENLX loop	Enable NT8D17 Conf/TDS/MFS card on loop and loop - 1. Enables all functions on the NT8D17 Conference/TDS card. Both the even numbered TDS/MFS loop and adjacent conference loop are enabled, where: loop = 1, 3, 5,... 255, System with Fibre Network Fabric If one of the loops is already enabled, it is disabled and then both loops are enabled. The Conf/TDS card is not enabled automatically when it is inserted. This command initiates card tests, downloads software and can be used in LD 34, LD 38 and LD 46. The DISL and ENLL commands can be used on the even number loop for the conference function. However, this only prevents the loop from being used by software and does not affect the hardware status of the card. The DISX and ENLX commands are recommended. Enabling more than 16 conference loops may cause the system to lock-up.	xct-15 fnf-25
LCNF loop	List busy and disabled conferee groups on specified loop.	basic-1
STAT loop	Provide status of conference card or IP-based conference loop. Output format is: • `CNFC n DSBL n BUSY` = number of conference groups disabled and busy • `CHAN n DSBL n BUSY` = number of channels disabled and busy • `UNEQ` = card is not equipped in the system • `DSBL` = card is disabled in software	basic-1
	Output format for IP loop is: • `IPCNFC n DSBL n BUSY n REG` = number of IP conference groups disabled and busy and the registration status of the Media Services Controller Conference Controller, where: - 00 = Media Services Controller Conference Controller is not properly registered with the Call Server	basic-6.50

Command	Description	Pack/Rel
	- 16 = Maximum number of IP conferences are registered and available for use • `IPCHAN n DSBL n BUSY n REG` = number of IP channels disabled and busy and the registration status of the Media Services Controller Conference Controller, where: - 00 = Media Services Controller Conference Controller is not properly registered with the Call Server - 30 = Maximum number of IP channels are registered and available for use	
STAT c u	List conference card and group used by specified TN. (Small Systems and CS 1000S)	
STAT l s c u	Lists which conference card and conferee group is being used by the specified terminal number.	basic-1

Chapter 16: LD 39: Intergroup Switch and System Clock Generator Diagnostic

The Intergroup Switch (IGS) and System Clock Generator (SCG) or Clock Controller (CC) diagnostic applies to Multi Group systems. It is used to:

- determine the status of any Peripheral Signaling, Intergroup Switch (IGS), System Clock Generator (SCG) or Clock Controller (CC) card
- disable and enable any PS, IGS, SCG or CC card
- switch the system clock from one SCG or CC to another
- clear minor alarm indications and the maintenance display on the active CPU
- All SCG commands can be used for Clock Controllers, although LD 60 is normally used when DTI, CPI or PRI features are installed

Group, loop, and Peripheral Signaling card relationship

Group	Shelf	PS	Loops
0	0	0	0-15
0	1	1	16-31
1	0	2	32-47
1	1	3	48-63
2	0	4	64-79
2	1	5	80-95
3	0	6	96-111
3	1	7	112-127
4	0	8	128-143
4	1	9	144-159
5	0	10	160-175
5	1	11	176-191

Group	Shelf	PS	Loops
6	0	12	192-207
6	1	13	208-223
7	0	14	224-239
7	1	15	240-255

Fibre Network Fabric

During the process of enabling FIJI card, the following tests will be performed:

- I/O test
- Check card ID
- Check Control Status Register
- Connection memory test for FIJI card
- Synchronize connection memory for active calls in that group

If the card passes the tests, it will be enabled; otherwise, proper error message will be printed.

The Fibre Network Fabric extends and enhances the 5-group network architecture to 8 non-blocking (inter-group) Network groups, with a resulting expansion in network capacity to 8k timeslots available for Intergroup traffic. This is achieved by using OC-12 SONET rings, and adding additional network and IPE shelves, cards and cables and software changes to allow using the expanded network capacity. This expansion increases the number of available loops from 160 to 256. This applies to Multi Group systems only.

Basic commands

ARCV ON/OFF	Set or reset auto-recovery operation for ring
ALRD x	Turn alarm display on or off for all FIJI cards.
CDSP	Clear the maintenance display on active CPU to 00 or blank
CMIN	Clears minor alarm for all customers
CMIN ALL	Clears minor alarm for all customers
DIS ALRM x y (z)	Disable alarm z (all) for FIJI in group x, side y

DIS FIJI x y	Disables FIJI in group x, side y
DIS IGS x	Disables IGS card x (0 to 19)
DIS RALM	Disable all alarms for all FIJI cards in ring x
DIS RING x	Disables all FIJI cards on side x
DIS SCG x	Disable SCG card x (0 or 1)
DISI IGS x	Disables IGS card x (0 to 19) when idle
DSPS x	Disable PS card x
END	Stop current operation or test
ENL ALRM x y (z)	Enable alarm z (all) for FIJI in group x, side y
ENL FIJI x y	Enables FIJI in group x, side y
ENL FIJI x y FDL	Enables FIJI in group x, side y with Force download.
ENL IGS x	Enables IGS card x (0 to 19)
ENL RALM x	Enable all alarms for all FIJI cards in ring x
ENL RING x	Enables all FIJI cards on side x
ENL SCG x	Enable SCG x (0 or 1)
ENPS x	Disable PS card x
IDC x y	Get cardid of FIJI card in group x, side y
RSET	Reset threshold for switchover functionality.
RSTR	Restore Ring(s)
SCLK	Switch clock to other SCG
SCLK FRCE	Force clock to switch to other SCG
STAT ALRM x y	Query alarm condition for FIJI card in group x, side y
STAT ALRM x y FULL	Query status of all alarms (active and inactive) for FIJI card in group x, side y
STAT FIJI x y	Get status of FIJI card in group x, side y
STAT FIJI x y FULL	Get status of FIJI card in group x, side y and display the card ID, firmware versions, and SONET status.
STAT IGS x	Get status of IGS card x (0 to 19)

STAT PER x	Print status of PS card x
STAT RING x	Get status of FIJI cards on side x
STAT SCG x	Print status of SCG x (0 or 1)
SWRG y	Switch call processing to ring y
TEST 360 x y z	Perform 360 test on FIJI card in group x (0-7), side Y (0 or 1) for time z (in 2 second intervals)
TEST ALL	Perform FIJI diagnostic test
TEST BKPL x y	Perform Backplane Test on Group X, Side Y
TEST CMEM x y	Perform Connection Memory test on the FIJI in group x (0-7) side y (0 or 1).
TEST FIJI x y	Self-test FIJI card in group x (0-7), side y (0-1)
TEST LINK Gt Gr S <D>	
	Perform Link test to identify FIJI hardware faults and speechpath problems

Alphabetical list of commands

Command	Description	Pack/ Rel
ARCV ON/OFF		fnf-25
	Set or reset auto-recovery operation for ring	
ALRD x	Alarm display for all FIJI cards where x = ON or OFF	fnf-25
CDSP	Clear the maintenance display on active CPU to 00 or blank.	basic-1
CMIN	Clears minor alarm for all customers	alrm_filter-22
CMIN ALL	Clears minor alarm for all customers	basic-1
DIS ALRM x y (z)		fnf-25
	Disable alarm z (all) for FIJI in group x, side y	
DIS FIJI x y	Disables FIJI in group x (0-7), side y (0-1)	fnf-25
DIS IGS x	Disables IGS card x (0 to 19).	basic-1

Command	Description	Pack/ Rel
DIS RING x	Disable all FIJI cards on side x (0-1)	fnf-25
DIS SCG x	Disable SCG card x (0 or 1). Not applicable for NTRB53 Clock Controller. Use LD 60 instead.	basic-1 basic-25.4
DISI IGS x	Disables IGS card x (0 to 19) when idle. Use of this command is recommended instead of DIS IGS, which interrupts calls in progress. The command's progress can be monitored by using the appropriate STAT command. The command's completion is indicated by an output of ISR043 on the maintenance terminal.	basic-1
DSPS x	Disable PS card x (0 to 15). Where: x = 0-15, System with Fibre Network Fabric	basic-1 fnf-25
END	Stop current operation or test.	basic-1
ENL ALRM x y (z)	Enable alarm z (all) for FIJI in group x (0-7), side y (0-1)	fnf-25
ENL FIJI x y	Enables FIJI in group x (0-7), side y (0-1)	fnf-25
ENL FIJI x y FDL	Enables FIJI in group x (0-7), side y (0-1) with Force download.	fnf-25
ENL IGS x	Enables IGS card x (0 to 19).	basic-1
ENL RING x	Enables all FIJI cards on side x (0-1)	fnf-25
ENL SCG x	Enable SCG x (0 or 1). Not applicable for NTRB53 Clock Controller. Use LD 60 instead.	basic-1 basic-25.4
ENPS x	Disable PS card x (0 to 15).	basic-1
IDC x y	Get cardid of FIJI card in group x (0-7), side y (0-1)	fnf-25
RSET	Reset threshold for switchover functionality.	fnf-25
RSTR	RestoreRing(s). Restore the rings to the best possible state (best to worst) as follows:	fnf-25

Command	Description	Pack/ Rel
	• Both Rings DRIVES HALF (Normal state) • Ring 1 DRIVES FULL - Ring 0 DRIVES NONE • Ring 0 DRIVES FULL - Ring 1 DRIVES N0NE • SURVIVAL state **Note:** This command can be issued with the rings in any state other than normal (DRIVES HALF)	
SCLK	Switch clock to other SCG. Functions with NTRB53 Clock Controller **Note:** Wait 2 to 3 minutes between clock switches. Ensure both clock controllers are locked by using SSCK (LD 60) before a manual clock switch is performed.	basic-1 basic-25.4
SCLK FRCE	Force clock to switch to other SCG. Functions with NTRB53 Clock Controller **Note:** Switch occurs regardless of 1 minute clock switch timer being set, or a FIJI alarm preventing a switch is on.	basic-3.0
STAT ALRM x y	Query alarm condition for FIJI card in group x, side y. This will display current state of alarms and whether they are disabled or not.	fnf-25
STAT ALRM x y FULL	Query status of all alarms (active and inactive) for FIJI card in group x, side y If the X parameter is omitted, the individual alarm status for each FIJI in ring Y is printed, with inactive (OFF) alarms suppressed. **Note:** The NEWK and NEWZ alarms are always printed. If both X and Y parameters are omitted, the alarm status is printed out for both rings.	fnf-25

Command	Description	Pack/ Rel
STAT FIJI x y	Get status of FIJI card in group x (0-7), side y (0-1). The FIJI card status and the number of busy junctors will be displayed. **Note:** x and y are optional parameters.	fnf-25
STAT FIJI x y FULL	Get status of FIJI card in group x (0-7), side y (0-1). The FIJI card status, the number of busy junctors, the card ID, the firmware versions, and the SONET status will be displayed. **Note:** x and y are optional parameters.	fnf-25
STAT IGS x	Get status of IGS card x (0 to 19). The response of "`x DSBL y BUSY`" indicates the number of junctor timeslots disabled or busy associated with the specified IGS card.	basic-1
STAT PER x	Print status of PS card x (0 to 9). Possible responses: • `DSBL: NOT RESPONDING` = PS card x is either missing, faulty or disabled via the faceplate switch. If there is a fault in the extender pair for the network shelf, the status of the PS card will also be DSBL: NOT RESPONDING. • `DSBL: RESPONDING` = The PS card is disabled and responding to the CPU. The PS may have been disabled by manual request (DSPS) or the associated extender pair may have been manually disabled. If neither of these conditions exist, the card may have been disabled because of an overload condition on the associated shelf. Check for OVD messages appearing in previous TTY output. An attempt to enable a PS card which was disabled because of an overload may result in a recurrence of the overload condition: the system's service may be impaired for approximately 2 minutes. Where: x = 0-15, System with Fibre Network Fabric	basic-1 fnf-25

Command	Description	Pack/ Rel
STAT RING x	Get status of Ring on Side X (0 to 1). State of RING and state of FIJI cards will be displayed. How many times a switchover took place will be displayed.	fnf-25
STAT SCG x	Print status of SCG x (0 or 1). Prints normal status of NTRB53 (not full status)	basic-1 basic-25.4
SWRG y	Switch call processing to ring y (0 to 1). This makes ring y drive all 960 inter-group timeslots.	fnf-25
TEST 360 x y z	Perform 360 test on FIJI card in group x (0-7), side y (0 or 1) for time z (in 2 second intervals) **Note:** The 360 test sends a test pattern on timeslot 1 thru all FIJI cards on the ring and back to the sending FIJI testing transmission through the whole ring. Output represents success or fail for links 0-7, 8-15, 16-23, 24-31. Example `000000FF` indicates failure on links 0-7.	fnf-25
TEST ALL	Perform FIJI diagnostic test. **Note:** Checks all FIJI cards in the system for FIJI hardware faults and speech path problems. The diagnostic test can also be added to the daily routine by adding LD 39 to the DROL prompt in LD 17.	basic-3.0
TEST BKPL x y	Perform Backplane test on group x, side y. The specified FIJI card writes a specific pattern to the backplane and reads it back. Result: Each link (0-31) is displayed with PASS or FAIL	fnf-25
TEST CMEM x y	Perform Connection Memory test on the GFIJI in group (0-7) side y (0 or1). Card must be in disable state.	fnf-25
TEST FIJI x y	Self-test FIJI card in group x (0-7), side y (0-1)	
TEST LINK Gt Gr S <D>	Perform Link test to identify FIJI hardware faults and speechpath problems, where:	basic-3.0

Command	Description	Pack/ Rel
	• Gt = the transmitting group • Gr = the receiving group • S = the side • <D> = the duration parameter in seconds (maximum 10 seconds). If not entered, a default duration is used. Result: Each link (0-31) is displayed with PASS or FAIL	

Chapter 17: LD 43: Equipment Datadump

This program is used to keep data on the system storage device up to date. When the datadump program is invoked, data in the read/write memory (including any that has been changed or added) is written to the storage device at the reserved (or specified, for a Co-resident CS and SS configuration) location reserved for it.

The program can be invoked daily as part of the daily routines or loaded manually. An incremental datadump occurs during the daily routines if database changes have been made.

Options 61C, and 81C utilize two CMDUs and disk redundancy, LD 43 commands apply to both sides of the system. Refer to the specific commands for the differences between Options 61C, or 81C and other systems. For general information, see *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning, NN43021-310* .

Following a successful EDD on Options 61C, and 81C, the "HI" (Hardware Infrastructure) string is output.

DATADUMP COMPLETE is output after completing the data dumps and backups to Z Drive.

DATADOWNLOAD COMPLETE is output after the databases are sent to the SIPE cabinets.

When the datadump fails

In the event of an unsuccessful initial dump, the office data on the tape or disk is suspect. Another datadump with spool option should be done on the same tape or disk; if successful, a transient error is indicated and normal procedures can be resumed. If this second attempt also fails, DO NOT attempt another datadump until the fault is isolated and corrected.

If the storage medium is not proved faulty and the storage device appears serviceable, datadumping to an OLD tape or disk, if available, may help to pinpoint the problem.

Except during the troubleshooting phase, storage medium which has failed to datadump successfully must not be left in the storage device. Should a SYSLOAD occur with such a storage medium, the load may terminate abnormally with unpredictable results.

Low memory warning

Unprotected data store equal in size to the length of the records being written (for example, 512 words) must be available to the datadump program.

A low memory warning message (SCH603) is issued when spare unprotected data store falls below a given threshold. Once this warning message has been issued, it is not possible to perform a datadump as the system requires spare unprotected data store equivalent to the size of a record on the storage medium (for example, 512 words).

Users should ensure that these amounts of spare unprotected data store are available before attempting to perform a datadump.

Basic commands

The following commands are applicable to Large System and CS 1000E Systems.

BKO xxx	Copy data from primary to backup device
BKR xx	Invoke database-replication operation.
DAT	Print the data issue and creation date of the primary and backup database
EDD EDD CLR EDD CN EDD DP xx xx ..xx EDD GP EDD HM EDD IWC EDD NBK EDD NS EDD NX EDD SA EDD SP EDD CCBR	Invoke datadump program Clear datadump inhibit flag Save CND names (use prior to datadump) Dump patch Get patch Save AWU, RMS and MR data (prior to dump) Inhibits write check: caution Inhibit database backup Inhibit tape far-end spool Write tape data records Complete data dump and bypass software audit Spool tape to far-end Invoke CCBR backup process
PBX CF6 (ALLOWED)	Bit dumped with PBX data block
RES xxx	Restore files to the primary device from the external backup device **Note:** This command requires a system INI for restored files to take effect.
RSR xx yy	Restore the database received from the primary system.
SWP	Swap (exchange) main and ".bak" data files on the primary flash drive

Alphabetical list of commands

Command	Description	Pack/Rel
BKO xxx	The file holding the MIB-II variables, System Navigation variables, and community name strings is copied from the primary device to the backup (external storage) device.	basic-19
	Where xxx = removable storage device type. • RMD = Compact Flash device • USB = USB memory stick **Note:** This parameter only applies when the Call Processor and SS applications are co-resident on a CP PM server.	basic-6.00
BKR xx	Invoke database-replication operation, where: xx = badkup rule number This command is typically entered on the primary system for replication to the secondary system.	grprim-4.0
DAT	Print the creation date of the main, secondary, or backup database.	basic-18
EDD	Invoke datadump program The Call Server MIB-II variables, System Navigation variables and community name strings are dumped to disk as a file when this command is executed. As well, this file is backed up to the A: drive floppy or to the internal Z: drive.	basic-1
	Invoke datadump program The Call Server data in the read/write memory (including data that has been changed or added) is written to the storage device at the reserved location as a file when the EDD command is executed. These files are backed-up to the following internal or external storage location:	basic-7.00

Command	Description	Pack/Rel
	• Removable Storage Media (Floppy Disk/Compact Flash or USB memory stick depends on the system platform) • Internal /u/ccbr directory as ccbr.gz file used for Customer Configuration Backup and Restore feature if CCBR option is included as part of the EDD command. **Important:** CCBR.GZ file is not generated during the default data dump. The CCBR.GZ file can be generated by using the EDD option command (EDD CCBR). • Internal /u/bkdb/backup directory as bkdata.gz file for Geographic Redundancy feature if Geographic Redundancy Primary Call Server Package (404) is equipped and ABKUP = IMM in Geographic Redundancy Data Base Replication Control (GRDRC in LD 117).	
EDD CLR	Clear datadump inhibit flag and do a datadump This flag is set because SYSLOAD or the conversion programs detect incomplete or inconsistent equipment data. Exercise caution since the use of this option may result in incorrect data being written.	basic-1
EDD CN	Save CND names. EDD CN saves the names associated with DNs for Caller's Name Display. Use Prior to datadump.	basic-1
EDD DP xx xx xx...	Dump patch Customer data and the specified patches (xx xx...xx) are dumped onto disk. If no patch numbers are specified, then only customer data is dumped.	basic-18
EDD GP	Get patches The non-patch customer data from the core memory is placed on the new disk without overwriting the preloaded patches on the disk. Any patches in the system are also ignored.	ph-6
EDD HM	Saves Automatic Wake Up (AWU), Room Status (RMS) and Message Registration (MR) data. Use prior to datadump, then system load. This should be performed prior to a SYSLOAD or software conversion.	basic-1

Command	Description	Pack/Rel
EDD IWC	Inhibits write check. Caution: for Emergency Use Only. Inhibits write check. This command is useful when the standard commands for datadump fail and end-of-file cannot be found. It writes an end-of-file on tape and allows other commands to be invoked.	basic-1
EDD NBK	Inhibit database backup. Indicates that a database backup should not be done after a datadump. (Applicable to hard disk storage with floppy disk backup).	basic-1
EDD NS	Inhibit tape far-end spool. Tape will not spool to the far-end and will not perform write test. Default option is SP. Overlay program cannot be aborted until writing has either been completed or has failed. This command applies to systems equipped with tape units.	basic-1
EDD NX	Writes tape data records consistent in size with predefined system values. Default option is NX.	basic-1
EDD SA	This command is used to complete the data dump and bypass the software audit of Peripheral Controller and superloop data.	basic-18
EDD SP	Spool tape to far-end. This command applies to systems equipped with tape units. Spools tape to the far-end in order to even the tension on the tape. Also writes a test record after the end of existing data to check for any write problems. If errors occur during test, data should remain intact.	basic-1
PBX CF6 (ALLOWED)		basic-1
	Bit dumped with PBX data block.	
RES xxx	The file created to store the MIB-II variables, System Navigation variables, and community name strings is restored from the backup (external storage) device to the primary device.	basic-19
	Where xxx = removable storage device type.	basic-6.00
	• RMD = Compact Flash device	
	• USB = USB memory stick	

Command	Description	Pack/Rel
	Note: This parameter only applies when the Call Processor and SS applications are co-resident on a CP PM server. **Note:** This command requires a system INI for restored files to take effect.	
RSR xx yy	Restore the database received from the primary system, where: • xx = backup rule number on the local system • yy = database version number (1). The latest database version is assigned the highest priority. For example: yy = 1 restores the latest backup database; yy = 2 restores the second latest database version. This command is typically entered on the secondary system to restore a database received from the primary system.	grsec-4.0
SWP	The new file created to store the MIB-II variables, System Navigation variables, and community name strings is swapped (exchanged) with the ".bak" file on the primary device.	basic-19

Chapter 18: LD 44: Software Audit

The audit program (LD 44) monitors system operation and provides an indication of the general state of system operation. The program is concerned mostly with the system software. When a software problem is encountered, the program outputs an AUD message and attempts to clear the problem automatically.

The audit program is changed to recognize and handle various scenarios added by Music or Recorded Announcement Broadcast features. The following checks are performed by audit for broadcasting trunks:

- Check the list of call registers connected to the broadcasting trunk and verify that the size of this list matches the number of callers connected according to the counter in the unprotected trunk block
- ensure that a trunk marked as broadcasting does indeed have more than one caller connected to it
- go through the list of call registers connected to the broadcasting trunk and ensure that the list is linked correctly from beginning to end
- all call registers in the broadcasting trunk call register list should point back to the broadcasting trunk
- various checks are done on the connections for a broadcasting call
- check through the list of call registers queued for and ensure the list is linked correctly from beginning to end

Running software audit

The Audit program is enabled as a Background Program or Daily Routine in the configuration record. See prompts BACKGROUND and DROL in LD 17. To load the Audit program manually, enter:

LD 44

R x

x is the number of audit passes required.

Enter 0 for continuous auditing. R and x must be separated by a space or the system responds with:

```
AUD REQ ERR.
AUDIT
```

The Meridian Mail MP data base audit (co-administration) is run during Audit if a data base mismatch is known by the system, or if it is being run manually.

Chapter 19: LD 45: Background Signaling and Switching Diagnostic

This program performs network continuity tests and outputs detected problems via BSD messages.

The Manual Continuity Test (MCT) allows you to isolate intermittent faulty points reported by the Background Continuity Test (BCT). For example, BCT reports faults between A, B, and C. Run the MCT between A and B, then between B and C to determine how often it fails.

When run in background, LD 45 tests the following on all enabled network loops:

- the continuity of the speech path between each network card and its associated IPE shelves is tested
- the continuity of the speech path between all network card is tested
- non functioning paths between network cards are identified

Note:
When running in background, only new faults detected are output.

Memory and signaling tests are only performed in LD 30. If LD 45 is included in background or midnight routines it is recommended that LD 30 also be included. By including LD 30, bad memory areas will be flagged before the continuity tests of LD 45 which will improve fault isolation.

On Small Systems and CS 1000S systems, this Overlay program is not available. Use Overlay program 30 (LD 30) to perform signaling tests on these systems.

Using the manual extended continuity (XCON) command

The XCON command is used to test various communication paths on or between NT8D04 Network, NT8D01 Controller, Multipurpose ISDN Signaling Processor (MISP), S/T-Interface Line (SILC) and U-Interface Line (UILC) cards. There are 10 paths XCON may test. Figure 6: XCON test paths on page 194 and Figure 7: XCON test paths (continued) on page 195 on Figure 7: XCON test paths (continued) on page 195 show 8 of these paths. Only 1 XCON test at a time can be run on a superloop.

To begin a manual extended continuity test, enter one of the following:

- XCON 0 = perform test once and output results
- XCON H hhh = repeat test for hhh hours (hhh = 1-255)
- XCON M mmm = repeat test for mmm minutes (mmm = 1-255)
- XCON S sss = repeat test for sss seconds (sss = 1-255)

After you enter a XCON command, you are prompted for a combination of the values listed below. The responses to these prompts determine the test performed.

Prompt — Response — Comment

DSLT — xx — Timeslot (2-31, 34-63, 66-95, 98-127) for Network Card associated with detector Controller.

GSLT — xx — Timeslot (2-31, 34-63, 66-95, 98-127) for Network Card associated with generator Controller.

JUNC — x — Junctor number (0-7).

LBTN — l s c u — Terminal Number (loop, shelf, card, unit) to be loopback point.

LBTY— N/P — Loopback address: N = Network Card, P = Controller or terminal.

Note:
When using XCON Test 9 for ISDN BRI, the possible responses for LBTY are 3 or 4. 3 indicated the test will take place with the DSL enabled; 4 performs the test with the DSL disabled.

PATT — x — Test pattern number (0-7). Signal sent by the generator to the detector. You should run a test several times with varying patterns.

SLOT — xx — Timeslot (2-31, 34-63, 66-95, 98-127). Enter return (<CR>) to select a random timeslot.

SUPL — l — Superloop number (0-156, in multiples of 4).

TAG — x — Tag number (1-15) returned by the system. Tag number 0 is used for one-shot tests (XCON 0).

TEST — x — Test case number (1-8).

TN — l s c u — Controller or terminal (loop, shelf, card, unit) to be the detector. For Controller, enter any valid TN on Controller's shelf. For special loopback channel enter: l s 99 0.

TYPD — N/P — Pattern detector: N = Network Card, P = Controller.

TYPG — N/P — Pattern generator: N = Network Card, P = Controller.

Fibre Network Fabric

The Fibre Network Fabric extends and enhances the 5-group network architecture to 8 non-blocking (inter-group) Network groups, with a resulting expansion in network capacity to 8k timeslots available for Intergroup traffic. This is achieved by using OC-12 SONET rings, and adding additional network and IPE shelves, cards and cables and software changes to allow using the expanded network capacity. This expansion increases the number of available loops from 160 to 256. This applies to Multi Group systems only.

For an existing fully configured machine (5 groups), the existing software takes about 4 hours to complete all 10080 inter-group continuity tests. When the number of groups grows from 5

to 8 and the number of junctors between any two groups grows to 32, the number of tests grows to 112896 which will take about 3 days and this is infeasible. The goal is to reduce the number of inter-group continuity tests to achieve the same diagnostic and maintenance functionalities within the same time frame.

With new hardware support, this new background continuity test for 8 groups can be done in parallel, instead of sequentially; however, the user interfaces remain unchanged.

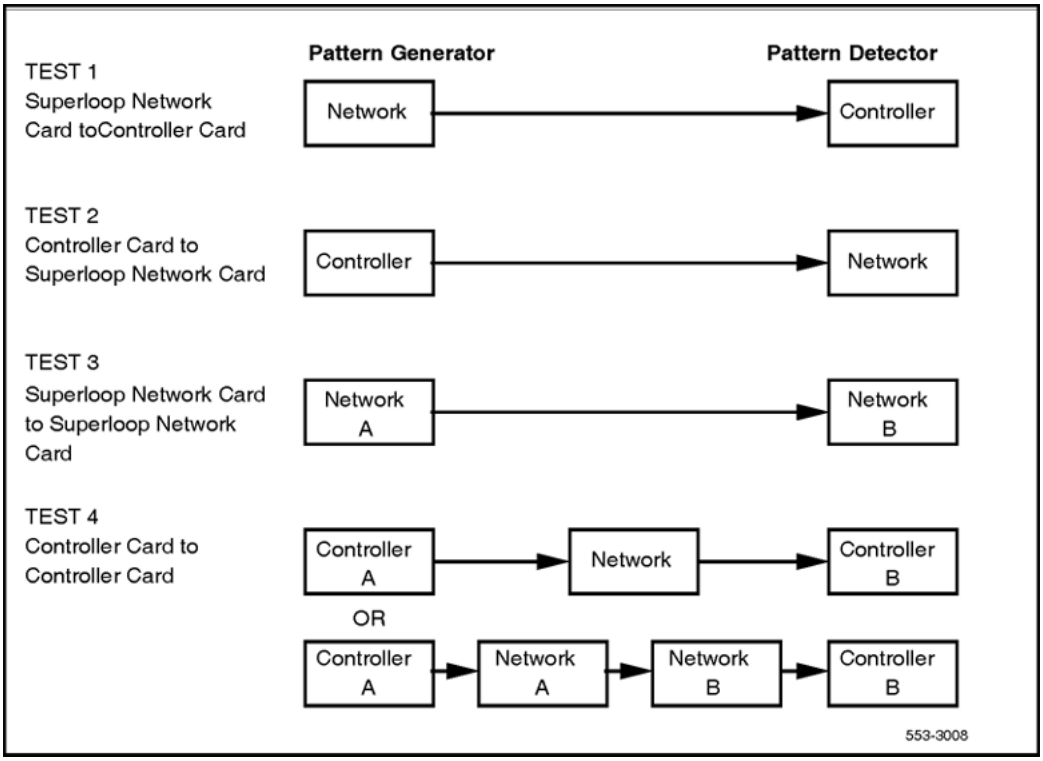


Figure 6: XCON test paths

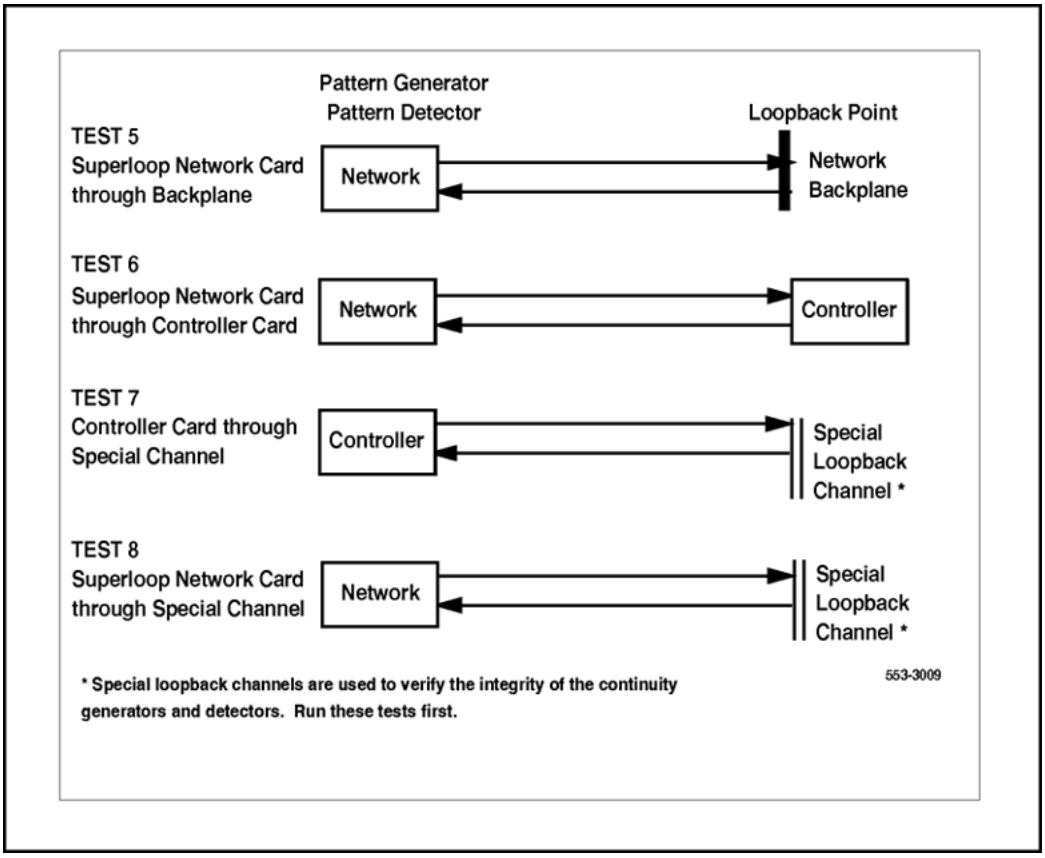


Figure 7: XCON test paths (continued)

Basic commands

TEST (loop)	Perform a complete continuity test for one or all loops. Unpluged cards are not tested for continuity.
XCON 0	Perform Extended Continuity test once and output results. User will be prompted for TEST number. XCON sub-prompts on page 196
XCON H hhh	Repeat Extended Continuity test for hhh hours (hhh = 1-255). User will be prompted for TEST number. XCON sub-prompts on page 196
XCON M mmm	Repeat Extended Continuity test for mm minutes (mm = 1-255). User will be prompted for TEST number. XCON sub-prompts on page 196
XCON S sss	Repeat Extended Continuity test for ss seconds (ss = 1-255). User will be prompted for TEST number. XCON sub-prompts on page 196

XINF	Display the tag numbers of all running and completed continuity tests
XSTA x	Get the status of manual continuity test with TAG = x
XSTP x	Stop manual continuity test with TAG = x

XCON sub-prompts

TEST = 1			
Test Path	Network Card to Controller. This test uses the Network Card (NT8D04) as a pattern generator and the Controller (NT8D01) as the detector.		Pack/Rel xpe-15
Prompt	Response	Description	
TEST	1	Network Card to Controller	
TYPE	SL	Test superloop (SL)	
PATT	x	Pattern (0-7)	
TYPG	N	Network Card is generator	
SUPL	loop	0-156 in multiples of 4	
SLOT	xxx	Timeslot 2-31, 34-63, 66-95, 98-127. SLOT appears if Remote IPE package 286 is not equipped.	
TYPD	P	Controller is detector E1 Carrier = Timesot : 0 = 5-31 ; 1 = 37-63 ; 2 = 69-95 T-1 Carrier = Timesot : 0 = 5-25 ; 1 = 37-57 ; 2 = 69-89	
TN	l s c u	Valid TN on the Controller	
TAG	xx	Tag number (1-15) assigned by the system	

TEST = 2			
Test Path	Controller to Network Card. This test uses the Controller (NT8D01) as a pattern generator and the Network Card (NT8D04) as the detector.		Pack/Rel xpe-15
Prompt	Response	Description	
TEST	2	Controller to Network Card	
PATT	x	Pattern (0-7)	
TYPG	P	Controller is generator	
TN	l s c u	Valid TN on the Controller	

TEST = 2		
TYPD	N	Network Card is detector
SUPL	loop	0-156 in multiples of 4
SLOT	xxx	Timeslot 2-31, 34-63, 66-95, 98-127
TAG	xx	Tag number (1-15) assigned by the system

TEST = 3			
Test Path	Network Card to different Network Card. This test uses the Network Card (NT8D04) as a pattern generator and another Network Card as the detector.		Pack/Rel xpe-15
Prompt	Response	Description	
TEST	3	Network Card to different Network Card	
PATT	x	Pattern (0-7)	
TYPG	N	Network Card is generator	
SUPL	loop	0-156 in multiples of 4	
SLOT	xxx	Timeslot 2-31, 34-63, 66-95, 98-127	
TYPD	N	Network Card is detector	
SUPL	loop	0-156 in multiples of 4	
SLOT	xxx	Timeslot 2-31, 34-63, 66-95, 98-127	
JUNC	x	Junctor if Network cards in different groups	
TAG	xx	Tag number (1-15) assigned by the system	

TEST = 4			
Test Path	Controller to different Controller. This test uses a Controller (NT8D01) as a pattern generator and another Controller as a detector. The pattern is sent through one or two Network Cards (NT8D04).		Pack/Rel xpe-15
Prompt	Response	Description	
TEST	4	Controller to different Controller	
PATT	x	Pattern (0-7)	
TYPG	P	Controller is generator	
TN	l s c u	Valid TN on the Controller	
TYPD	P	Controller is detector	
TN	l s c u	Valid TN on the Controller	
GSLT	xxx	Timeslot 2-31, 34-63, 66-95, 98-127 on generator Network Card	

TEST = 4		
DSLT	xxx	Timeslot 2-31, 34-63, 66-95, 98-127 on detector Network Card
JUNC	x	Junctor if Network cards in different groups
TAG	xx	Tag number (1-15) assigned by the system

TEST = 5		
Test Path	Network Card to Network Card (loop back at backplane). This test uses the Network Card (NT8D04) as a pattern generator and detector. The pattern is sent to the network backplane and back.	Pack/Rel xpe-15
Prompt	Response	Description
TEST	5	Network Card to Network Card (loop back at backplane)
PATT	x	pattern (0-7)
TYPG	N	Network Card is generator
SUPL	loop	0-156 in multiples of 4
SLOT	xxx	timeslot 2-31, 34-63, 66-95, 98-127
TYPD	N	Network Card is detector
SUPL	loop	0-156 in multiples of 4
SLOT	xxx	timeslot 2-31, 34-63, 66-95, 98-127
LBTY	N	through network backplane
TAG	xx	tag number (1-15) assigned by the system

TEST = 6		
Test Path	Network Card to Network Card (loop back through Controller). This test uses the Network Card (NT8D04) as a pattern generator and detector. The pattern is looped back through a Controller (NT8D01).	Pack/Rel xpe-15
Prompt	Response	Description
TEST	6	Network Card to Network Card (loop back through Controller)
PATT	x	Pattern (0-7)
TYPG	N	Network Card is generator
SUPL	loop	0-156 in multiples of 4
SLOT	xxx	Timeslot 2-31, 34-63, 66-95, 98-127
TYPD	N	Network Card is detector
SUPL	loop	0-156 in multiples of 4

TEST = 6		
SLOT	xxx	Timeslot 2-31, 34-63, 66-95, 98-127
LBTY	P	Through Controller
LBTN	l s 99 0	Special Controller loop back channel
TAG	xx	Tag number (1-15) assigned by the system

TEST = 7			
Test Path	Controller to Controller (special loop back channel). This test uses the Controller (NT8D01) as a pattern generator and detector. The pattern is looped back through a special loop back channel.		Pack/Rel xpe-15
Prompt	Response	Description	
TEST	7	Controller to Controller (special loop back channel)	
PATT	x	Pattern (0-7)	
TYPG	P	Controller is generator	
TN	l s 99 0	Special Controller loop back channel	
TAG	xx	Tag number (1-15) assigned by the system	

TEST = 8			
Test Path	Network Card to Network Card (special loop back channel). This test uses the Network Card (NT8D04) as a pattern generator and detector. The pattern is looped back through a special channel which is specified by timeslot 128.		Pack/Rel xpe-15
Prompt	Response	Description	
TEST	8	Network Card to Network Card (special loop back channel)	
PATT	x	Pattern (0-7)	
TYPG	N	Network Card is generator	
SUPL	loop	0-156 in multiples of 4	
SLOT	128	Special Network loop back channel	
TAG	xx	Tag number (1-15) assigned by the system	

TEST = 9		
Test Path	Loop back test on Digital Subscriber Loop. This test uses the MISP as a pattern generator and detector. The pattern goes through the Network and Controller Card and is looped back at a single DSL. Both B- and D-channels are looped back.	Pack/Rel bri-18

TEST = 9		
Prompt	Response	Description
TEST	9	Loop back test on Digital Subscriber Loop
PATT	x	Pattern (0-7)
TYPG	N	Network Card is generator
SUPL	loop	0-156 in multiples of 4
SLOT	128	Special Network loop back channel
LBTY	3	DSL is requested for loop back
LBTN	l s c d	Address of DSL
TAG	xx	Tag number (1-15) assigned by the system

TEST = 10			
Test Path	Loop back test on BRI line card. This test uses the MISP as a pattern generator and detector. The pattern goes through the Network and Controller Card and is looped back at the line card level (i.e., bus loop back). Both B- and D-channels are looped back.		Pack/Rel bri-18
Prompt	Response	Description	
TEST	10	Loop back test on BRI line card	
PATT	x	Pattern (0-7)	
TYPG	5	MISP is generator	
SUPL	loop	0-156 in multiples of 4	
SLOT	128	Special Network loop back channel	
LBTY	4	loop back at line card	
LBTN	l s c d	Address of DSL	
TAG	xx	Tag number (1-15) assigned by the system	

Alphabetical list of commands

Command	Description	Pack/Rel

Command	Description	Pack/Rel
TEST (loop)	Perform a complete continuity test for one or all loops. Performs a complete test and reports all faults detected (even if they have been previously reported), where: loop = 0-225, System with Fibre network Fabric	basic-1 fnf-25
XCON 0	Perform Extended Continuity test once, then output results. After entering this command, you will then be able to select and conduct 1 of 10 possible XCON tests. These XCON tests begin on XCON sub-prompts on page 196.	xpe-15
XCON H hhh	Perform Extended Continuity test for hhh (1-255) hours, then output results. After entering this command, you will then be able to select and conduct 1 of 10 possible XCON tests. These XCON tests begin on XCON sub-prompts on page 196.	xpe-15
XCON M mmm	Perform Extended Continuity test for mmm (1-255) minutes, then output results. After entering this command, you will then be able to select and conduct 1 of 10 possible XCON tests. These XCON tests begin on XCON sub-prompts on page 196.	xpe-15
XCON S sss	Perform Extended Continuity test for sss (1-255) seconds, then output results. After entering this command, you will then be able to select and conduct 1 of 10 possible XCON tests. These XCON tests begin on XCON sub-prompts on page 196.	xpe-15
XINF	Display the tag numbers of all running and completed tests. The output format (where T# = Tag Number) is: `RUNNING: T# T# T# T#. . . . DONE: T# T# T# T#. . . . SUSPENDED: T# T# T# T#. . . . FREE: x x` (number of free tags available [0-15])	xpe-15
XSTA x	Get the status of manual continuity test with TAG = x. Individual tests are identified by the tag number the system generates when you complete a sequence of test prompts. See also the XINF and XSTP commands. The test status provides the following format information: PATT x — Pattern number GENERATE: — Generator information follows: TYPG N/P — Network or Controller as pattern generator	xpe-15

Command	Description	Pack/Rel
	SUPL x Superloop number or TN on Controller	
	SLOT x Timeslot	
	DETECT: Detector information follows:	
	TYPD N/P Network or Controller as pattern detector	
	SUPL x Superloop number or TN on Controller	
	SLOT x Timeslot	
	RESULTS: Results follow:	
	TESTS COMPLETED: xxxxxxxx	
XSTP x	Stop manual continuity test with TAG = x. Individual tests are identified by the tag numbers. The XSTP command outputs the test status. See also XINF and XSTA commands.	xpe-15

Alphabetical list of XCON sub-prompts

Prompt	Response	Description
DSLT	xxx	Timeslot (2-31, 34-63, 66-95, 98-127) for Network Card associated with detector Controller
GSLT	xxx	Timeslot (2-31, 34-63, 66-95, 98-127) for Network Card associated with generator Controller
JUNC	x	Junctor number (0-7) Where: x = 0-31, System with Fibre Network Fabric
LBTN	l s c u l s c d	Loop back Controller or Terminal Number. Where: l = loop, s = shelf, c = card, u = unit, and d = Digital Subscriber Loop (DSL).
LBTY	y	Loop back Type (3, 4, N, or P). Where: • 3 = Digital Subscriber Loop • 4 = Line Card • N = Network Card • P = Controller or Terminal

Prompt	Response	Description
PATT	x	Test pattern (0-7) sent by the generator to the detector
SLOT	xxx	Timeslot (2-31, 34-63, 66-95, 98-127). Enter return (<CR>) to select a random timeslot. For special loop back slot enter: 128.
SUPL	loop	Superloop number in multiples of 4, where: • loop = 0-156 • loop = 0-252, System with Fibre Network Fabric
TAG	xx	Tag number (0-15) returned by the system. Tag number 0 is used for one-shot tests (XCON 0).
TEST	xx	XCON test path (1-10). Where: • 1 = Network Card to Controller • 2 = Controller to Network Card • 3 = Network Card to different Network Card • 4 = Controller to different Controller • 5 = Network Card to Network Card (loop back at backplane) • 6 = Network Card to Network Card (loop back through Controller) • 7 = Controller to Controller (special loop back channel) • 8 = Network Card to Network Card (special loop back channel) • 9 = Loop back test on Digital Subscriber loop • 10 =Loop back test on BRI line card
	xxx	Perform a complete continuity test for one or all loops. Performs a complete test and reports all faults detected (even if they have been previously reported), where: xxx = 0-255, System with Fibre Network Fabric
TN	l s c u	Controller or terminal (loop, shelf, card, unit) to be the detector. For Controller, enter any valid TN on Controller's shelf. For special loop back channel enter: l s 99 0.

Prompt	Response	Description
		Where: l = 0-255, System with Fibre Network Fabric
TYPD	y	Type of Pattern Detector (N or P). Where: N = Network Card and P = Controller.
TYPG	y	Type of Pattern Generator (5, N, or P). Where: • 5 = Multipurpose ISDN Signaling Processor • N = Network Card • P = Controller

Chapter 20: LD 46: Multifrequency Sender Diagnostic for Automatic Number Identification

This program is used to maintain the Multifrequency Sender card. The Multifrequency Sender card provides multifrequency signals of Automatic Number Identification (ANI) digits over Centralized Automatic Message Accounting (CAMA) trunks to a toll switching CAMA, Traffic Operator Position System (TOPS) or Traffic Service Position System (TSPS).

The MFS diagnostic program can be run in background, during the daily routines, or manually to enter commands. It performs the following tests:

- checks that the MF Sender card responds to system I/O functions
- tests the 30-channel memory locations, the 480 (30 x 16) digit buffer memory locations and the 64 First-in, First-out locations
- exercises all 15-digit codes with digit strings from 2 to 16 digits long and verifies both the 68 ms pulse width and whether each string outpulses to completion

No check is possible on MFS frequencies used in each tone burst due to the lack of receivers in the system. Also, no check can be made as to whether the correct digits are being outpulsed.

Overlay 46 is not supported on Small Systems and CS 1000S systems.

Fibre Network Fabric

The Fibre Network Fabric Expansion extends and enhances the 5-group network architecture to 8 non-blocking (inter-group) Network groups, with a resulting expansion in network capacity to 8k timeslots available for Intergroup traffic. This is achieved by using OC-12 SONET rings, and adding additional network and IPE shelves, cards and cables and software changes to allow using the expanded network capacity. This expansion increases the number of available loops from 160 to 256. This applies to Multi Group systems only.

Basic commands

CDSP CMAJ CMIN CMIN ALL	Clear the maintenance display on active CPU to 00 or blank Clear major alarm and reset power fail transfer Clears minor alarm for all customers. Clears minor alarm for all customers.
DISL loop DISX loop	Disable MFS loop Disable Conf/TDS/MFS card on loop and loop + 1
END ENLL loop ENLX loop	Stop all current testing Enable loop Enable Conf/TDS/MFS card on loop and loop + 1
MFS loop	Test and enable MFS loop
STAT loop	Get status of MFS loop
TONE loop TONE loop ALL	Enter input mode to provide MF tone bursts Provide MF tone bursts for all digits on specified loop

Alphabetical list of commands

Command	Description	Pack/Rel
CDSP	Clear the maintenance display on active CPU to 00 or blank.	basic-1
CMAJ	Clear major alarm, reset power fail transfer and clear power fault alarm.	basic-1
CMIN	Clears minor alarm for all customers.	alrm_filter-22
CMIN ALL	Clears minor alarm for all customers.	basic-1
DISL loop	Disable MFS loop. For NT8D17 Conference/TDS/MFS cards, see ENLL command, where:	basic-1
	loop = 0-254, System with Fibre Network Fabric	fnf-25

Command	Description	Pack/Rel
DISX loop	Disable NT8D17 Conference/TDS/MFS card on loop and loop + 1.	xct-15
	Disables the entire combined Conference, Tone and Digit Switch, and MF Sender (XCT) card. Both the even numbered TDS/MFS loop and adjacent conference loop are disabled, where:	
	loop = 0, 2, 4,. . . 254, System with Fibre Network Fabric	fnf-25
	The DISL and ENLL commands can be used on the even number loop for the TDS/MFS functions. However, this only prevents the loop from being used by software and does not affect the hardware status of the card. The ENLX and DISX commands are recommended. The ENLX command must be used if the DISX command was used to disable the card. This command can be used in LD 34, LD 38 and LD 46, where:	
	loop = 0-254, System with Fibre Network Fabric	fnf-25
END	Stop all current testing.	basic-1
ENLL loop	Enable loop.	basic-1
	For NT8D17 Conference/TDS/MFS cards the DISX and ENLX commands must be used whenever the faceplate switch of the card has been toggled. ENLL will software enable the card but the card will not be properly reset, where:	
	loop = 0-255, System with Fibre Network Fabric	fnf-25
ENLX loop	Enable NT8D17 Conference/TDS/MFS card on loop and loop + 1.	xct-15
	Enables all functions on the NT8D17 Conference/TDS card. Both the even numbered TDS/MFS loop and adjacent conference loop are enabled, where:	
	loop = 0, 2, 4. . . 254, System with Fibre Network Fabric	fnf-25
	If one of the loops is already enabled, it is disabled and then both loops are enabled. Enabling more than 16 conference loops may cause system to lock-up. This command initiates card tests, downloads software and can be used in LD 34, LD 38 and LD 46.	fnf-25

Command	Description	Pack/Rel
	The DISL and ENLL commands can be used on the even number loop for the TDS/MFS functions. However, this only prevents the loop from being used by software and does not affect the hardware status of the card. The ENLX and DISX commands are recommended, where: loop = 0-254, System with Fibre Network Fabric The Conf/TDS card is not enabled automatically when it is inserted.	
MFS loop	Test and enable MFS loop.	basic-1
STAT loop	Get status of MFS loop. Response is: • `LOOP UNEQ` —loop is unequipped • `LOOP DSBL` —loop is disabled • `CHAN yy` —number of channels busy • `xx DSBL yy BUSY` —number of channels disabled & busy • `NOT MFS` —loop is not an MFS loop Where: loop = 0-255, System with Fibre Network Fabric	basic-1 fnf-25
TONE loop	Enter input mode to provide MF tone bursts.	basic-1
TONE loop ALL	Provide MF tone bursts for all digits on specified loop (1 to 9, 0, 11 to 15, in that order).	basic-1

Chapter 21: LD 48: Link Diagnostic

The Link Diagnostic program is used to maintain data links used with various special features and auxiliary data links. A maintenance telephone cannot use LD 48.

Automatic Call Distribution Links

When equipped with the Automatic Call Distribution (ACD) feature, the system is supplemented with an Auxiliary Data Store (ADS) minicomputer system. The auxiliary data processor is located external to the system and is connected via a high-speed link and a low-speed link.

The high-speed link is used for transmission of ACD-related messages between the system and the auxiliary processor; the low-speed link is used for transmission of maintenance/error messages between the maintenance TTY (connected to the system) and the auxiliary processor.

Note:
When enabling a high-speed link (using the command "ENL HSL" or "ENL SDI HIGH" in LD 48), the craftsperson must log out of the TTY to receive a message from the system which confirms that the high-speed link (HSL) has been enabled.

Each Auxiliary Processor Link (APL) consists of a single Serial Data Interface (SDI) port connected via an interface cable to an interface port on the auxiliary processor.

ACD High speed and low speed link monitor

The ACD monitor diagnoses messages which flow across the link. This tool is useful to someone experienced with message formats and protocols.

APL monitor

The APL monitor is a tool used to diagnose the messages flowing across the link. This is only useful for someone experienced with the message formats and protocols.

Integrated Messaging System Links

The link maintenance capabilities provided for Integrated Messaging System (IMS) and Integrated Voice Messaging System (IVMS) links allow the link to be disabled/enabled and put into the maintenance mode.

The link software/hardware status can also be displayed. The program allows the craftsman to request that the printouts of all packed and/or unpacked messages be sent over a specified APL link.

Using print options (packed/unpacked messages) and observing the patterns of messages sent over the link, the most probable fault location (AUX, Meridian 1/Meridian SL-1 or SDI cable) can be determined.

Command and Status Links (CSL)

The Command and Status Link is an application protocol used for communication between the Meridian 1/Meridian SL-1 CPU and an external Value Added Server such as the Meridian Mail MP. The CSL runs on an Enhanced Serial Data Interface (ESDI) card.

In addition to the tests in LD 48, resident firmware diagnostics for the CSLs and ESDIs can output CSA, ESDA, ESDI error messages.

Multi-purpose Serial Data Link (MSDL)

MSDL provides 4 ports for applications such as ISDN Primary Rate D-channels (DCH) and Application Module Links (AML) and SDI functions.

The MSDL commands are listed below, where x is the MSDL device number (defined by prompt DNUM in LD 17). These are provided in Link Diagnostic (LD 48) and D-channel Maintenance (LD 96), and I/O Diagnostic (LD 37).

DIS MSDL x (ALL) — Disable MSDL card ENL MSDL x (FDL, ALL) — Enable MSDL card RST MSDL x — Reset MSDL card STAT MSDL (x (FULL)) — Get MSDL status SLFT MSDL x — Execute a self-test on MSDL card x

These are provided in Link Diagnostic (LD 48) and D-channel Maintenance (LD 96), and I/O Diagnostic (LD 37) Overlays.

Application Module Link (AML)

An Application Module Link (AML) provides a connection to applications such as Meridian Link. The AML is configured on an Enhanced Serial Data Interface (ESDI) or Multipurpose Serial Data Link (MSDL) card.

AML/CSL monitor

The AML monitor is a tool used to diagnose the messages flowing across the link. This is only useful for someone experienced with the message formats and protocols.

ISDN BRI monitor

This capability is used to monitor input/output messages to the MISP and SILC/UILC. This is only useful for someone experienced with the message formats and protocols. A password is required for DGB and MON options. The SETM TNx, RSET TNx and RSET ALL commands are also available for digital telephones.

Caution:
Use of the SETM MISP loop MON commands may use all system printing registers and cause an initialization.

Single Terminal Access (STA)

Single Terminal Access (STA) is an application available on the MSDL card. The STA application reduces the number of physical devices used to administer and maintain the system and its auxiliary processors.

Voice Mailbox Administration (VMBA)

Voice Mailbox Administration (VMBA) allows for Integrated Voice Mailbox Administration when using Meridian Mail.

Fibre Network Fabric

The Fibre Network Fabric extends and enhances the 5-group network architecture to 8 non-blocking (inter-group) Network groups, with a resulting expansion in network capacity to 8k timeslots available for Intergroup traffic. This is achieved by using OC-12 SONET rings, and adding additional network and IPE shelves, cards and cables and software changes to allow using the expanded network capacity. This expansion increases the number of available loops from 160 to 256. This applies to Multi Group systems only.

D-channel Expansion

With the introduction of D-channel Expansion, new software allows the increase of D-channels past sixty-four. Instead of the large system having a maximum of 16 I/O addresses, the new software allows 16 physical I/O addresses (0 - 15) per network group for D-channels defined on MSDL. With this enhancement a response to the system response GROUP is required to inform the system of the desired network group.

Basic commands

Contents

Section
ACD High speed and low speed link commands on page 217
ACD High speed and low speed link monitor commands on page 218
AML commands on page 218
AML over Ethernet (ELAN subnet) commands on page 219
AML/CSL monitor commands on page 220
Auxiliary Processor Link (APL) commands on page 221
APL monitor commands on page 222
D-channel Expansion commands on page 222

Section
Intercept Computer Update (ICU) commands on page 224 ISDN BRI monitor commands on page 225 Multipurpose Serial Data Link (MSDL) commands on page 226 Single Terminal Access (STA) commands on page 226 Voice Mailbox Administration (VMBA) commands on page 227

Basic commands

CMIN	Clears minor alarm for all customers.
CMIN ALL	Clears minor alarm for all customers.
DACR ALL x	Release ALL devices on Link x
DACR AGT l s c u	Release Agent
DACR RTE x y	Release Route x for Customer y
DIS AML x	Disable AML x
DIS AML x AUTO	Disable AUTO recovery on AML x (MSDL only)
DIS AML x LYR2	Disable layer two on AML x
DIS AML x LYR7	Disable layer seven on AML x
DIS AML x MDL	Disable MDL error reporting on AML x (MSDL only)
DIS AML x MON	Disable monitor on AML x (MSDL only)
DIS APL x	Put software AUX link x in maintenance mode
DIS HSL	Disable the high-speed link
DIS ICP x	Put ICP link x into maintenance mode
DIS ISDI x	Disable hardware AUX link SDI x
DIS MON	Disable the monitor-bit of high-speed link data
DIS MSDL x (ALL)	Disable MSDL device x
DIS MSGI x	Disable the MSGI option
DIS MSGO x	Disable the MSGO option
DIS PACI x	Disable the PACI option

DIS PACO x	Disable the PACO option
DIS PPRT x	Disable packet message print option on link x
DIS PRNT	Disable the print-bit of high-speed link data
DIS SDI HIGH	Disable the SDI port for high-speed link
DIS SDI LOW	Disable the SDI port for low-speed link
DIS STA x	Disable the STA application.
DIS UPRT x	Disable unpacket message print on AUX link x
DSC ESDI x	Disconnect the link
DSIC LSTI x	Disable printing of lost input messages on link x
DSIC LSTO x	Disable printing of lost output messages on link x
DSIC MSGI x	Disable printing of input messages on link x at input queue level
DSIC MSGO x	Disable printing of output messages on link x at output queue level
DSIC PACI x	Disable printing of input messages on link x at input buffer level
DSIC PACO x	Disable printing of output messages on link x at output buffer level
ENIC LSTI x	Enable printing of lost input messages on link x
ENIC LSTO x	Enable printing of lost output messages on link x
ENIC MSGI x	Enable printing of messages on link x at input queue level
ENIC MSGO x	Enable printing of messages on link x at output queue level
ENIC PACI x	Enable printing of input messages on link x at input buffer level
ENIC PACO x	Enable printing of output messages on link x at output buffer level
ENL AML x	Enable AML x
ENL AML x ACMS	Enable automatic set-up on AML x (ESDI only)
ENL AML x AUTO	Enable AUTO recovery on AML x (MSDL only)
ENL AML x FDL	Force download loadware to the MSDL card and enable AML x
ENL AML x LYR2	Enable layer two on AML x
ENL AML x LYR7	Enable layer seven on AML x
ENL AML x MDL	Enable MDL error reporting on AML x (MSDL only)
ENL AML x MON	Enable monitor on AML x (MSDL only)

EST AML x	Establish layer two on AML x
ENL APL x	Put software AUX link x in non-maintenance mode
ENL HSL	Enable the high-speed link
ENL ICP x	Enable ICP link x
ENL ISDI x	Enable AUX link SDI x
ENL MON	Print software information at maintenance TTY
ENL MSDL x (ALL, FDL)	Enable MSDL device x
ENL MSGI x	Print incoming messages from link x
ENL MSGO x	Print outgoing messages from link x
ENL PACI x	Print incoming messages from link x
ENL PACO x	Print outgoing messages from link x
ENL PPRT x	Enable packet message print option on link x
ENL PRNT	Connect high-speed link to TTY
ENL SDI HIGH	Enable SDI port for high-speed link
ENL SDI LOW	Enable SDI port for low-speed link
ENL UPRT x	Enable unpacked message print on link x
ENLX MSGI x p	Output incoming priority p messages from link x
ENLX MSGO x p	Output outgoing priority p messages from link x
ENL STA x (FDL)	Enable STA application. The MSDL card must be enabled to implement this command.
ICP ADD xxxx	Set up additional information xxxx to be used in the ICP message
ICP CLR	Clear previous ICP message set up without sending it
ICP DN xxxx	Set up ICP DN xxxx to be used in the ICP message
ICP IPN xx	Set up IPN number xx to be used in the ICP message
ICP LINK xx	Set up ICP link x to be used in the ICP message
ICP RSN x	Set up the intercept transfer reason x to be used in the ICP message
ICP SEND xx yy	Send the defined ICP message number xx, yy times
ICPM	Access ICP maintenance commands
MAP AML (x)	Get physical address and card name of one or all AMLs
MAP STA x	Get information relating to the STA application.

PSWD	Enter password to use ICP maintenance commands
RLS AML x	Release layer two on AML x
RSET ALL	Stop printing all messages on a line card
RSET BRIM	Stop printing of messages on SILC/UILC, MISP or digital line card
RSET IFx 1 PDL2 1	Stop printing SAPI 16 interface messages.
RSET IFx 1 PDNI n	Stop printing network interface messages.
RSET IFx l s c u BCH x	Stop printing B-channel terminal interface messages.
RSET IFx l s c u DCHx	Stop printing D-channel terminal interface messages.
RESET IMSG l s c dsl	Disable monitoring on incoming
RSET MISP loop AMO	Stop MISP printing of audit messages on MISP card
RSET MISP loop DGB	Exit MISP debug
RSET MISP loop MNT	Stop MISP printing of status messages on MISP card
RSET MISP loop MON	Stop printing of input/output messages on MISP card
RSET MPHM	Stop all Meridian Packet Handler message monitoring.
RSET OMSG l s c dsl	Disable monitoring on outgoing
RSET TNx	Stop printing messages on an ISDN BRI line card
RST MSDL x	Reset MSDL device x
SETM BRIM xxxx	Set printing of messages on SILC/UILC, MISP or digital line card
SETM IFx 1 PDL2 1	Set printing of SAPI 16 interface messages
SETM IFx 1 PDNI n	Set printing of network interface messages.
SETM IFx l s c u BCHx	Set printing of B-channel terminal interface messages.
SETM IFx l s c u DCHx	Set printing of D-channel terminal interface messages.
SETM IMSG l s c dsl MON x	Set monitor on incoming msg
SETM MISP loop AMO	Set printing of audit messages on MISP card
SETM MISP loop DBG	Set debug option on MISP card
SETM MISP loop MNT	Set printing of status messages on MISP card
SETM MISP loop MON	Set printing of input/output messages on MISP card
SETM MPHM xxxx	Set printing of Meridian Packet Handler messages. Where: xxxx = the MPHs to be monitored

SETM OMSG l s c dsl MON x	Set monitor on outgoing msg
SETM TNx l s c u, 31	Set printing messages on a digital line card unit (u) or ISDN BRI line card (31)
SETM TNx l s c u, dsl	Set printing messages on a unit
SLFT AML x	Invoke self-test for AML x
SLFT MSDL x	Invoke self-test for MSDL device x
STAT AML (x)	Get AML status
STAT APL x	Display status of AUX link x
STAT CNFG	Get status of link monitor/simulator configuration
STAT CSDI x	Get status of SDI port x
STAT DSP LNK x	Get status of all Displays on link x
STAT HSL	Get high-speed link status
STAT ICP (x)	Display software status of one or all ICP links
STAT ISDI x	Get status of hardware AUX link SDI x
STAT LSL	Get low-speed link status
STAT MON (x)	Get status of one or all message monitors
STAT MSDL (x [FULL])	Get MSDL status
STAT SDI HIGH	Get status of high-speed link port
STAT SDI LOW	Get status of low-speed link port
STAT STA x	Get status of STA application.
SWCH AML x y	Switch active (x) and standby (y) AML
UPLD AML x TBL x	Upload parameter Table 1 to 4 from AML x (MSDL only)

ACD High speed and low speed link commands

The following commands are used to enable, disable, test and check the status of an APL link.

Note:
When enabling a high-speed link (using the command "ENL HSL" or "ENL SDI HIGH" in LD 48), the craftsperson must log out of the TTY to receive a message from the system which confirms that the high-speed link (HSL) has been enabled.

DIS HSL	Disable the high-speed link
DIS SDI HIGH	Disable the SDI port for high-speed link
DIS SDI LOW	Disable the SDI port for low-speed link
ENL HSL	Enable the high-speed link
ENL SDI HIGH	Enable SDI port for high-speed link
ENL SDI LOW	Enable SDI port for low-speed link
STAT HSL	Get high-speed link status
STAT LSL	Get low-speed link status
STAT SDI HIGH	Get status of high-speed link port
STAT SDI LOW	Get status of low-speed link port

ACD High speed and low speed link monitor commands

The monitor is a tool used to diagnose the messages flowing across the link. This is only useful for someone experienced with the message formats and protocols.

DIS MON	Disable the monitor-bit of high-speed link data
DIS PRNT	Disable the print-bit of high-speed link data
ENL MON	Print software information at maintenance TTY
ENL PRNT	Connect high-speed link to TTY
STAT MON (x)	Get status of one or all message monitors

AML commands

The AML commands are listed below, where x is the AML logical device number (defined by prompt ADAN in LD 17). Some of these commands only apply to AMLs on an MSDL card.

DIS AML x	Disable AML x
DIS AML x AUTO	Disable AUTO recovery on AML x (MSDL only)
DIS AML x LYR2	Disable layer two on AML x
DIS AML x LYR7	Disable layer seven on AML x
DIS AML x MDL	Disable MDL error reporting on AML x (MSDL only)
DIS AML x MON	Disable monitor on AML x (MSDL only)
ENL AML x	Enable AML x
ENL AML x ACMS	Enable automatic set-up on AML x (ESDI only)
ENL AML x AUTO	Enable AUTO recovery on AML x (MSDL only)
ENL AML x FDL	Force download loadware to the MSDL card and enable AML x
ENL AML x LYR2	Enable layer two on AML x
ENL AML x LYR7	Enable layer seven on AML x
ENL AML x MDL	Enable MDL error reporting on AML x (MSDL only)
ENL AML x MON	Enable monitor on AML x (MSDL only)
EST AML x	Establish layer two on AML x
MAP AML (x)	Get physical address and card name of one or all AMLs
RLS AML x	Release layer two on AML x
SLFT AML x	Invoke self-test for AML x
STAT AML (x)	Get AML status
SWCH AML x y	Switch active (x) and standby (y) AML
UPLD AML x TBL x	Upload parameter table 1 to 4 from AML x (MSDL only)

AML over Ethernet (ELAN subnet) commands

DIS ELAN TEST	Disable ELAN subnet (server task)
DIS ELAN x TEST	Disable ELAN subnet link number x (client task)
ENL ELAN	Enable ELAN subnet (server task)
STAT ELAN	Check status of all configured ELAN subnets
STAT ELAN xxx	Check status of ELAN xxx

AML/CSL monitor commands

The AML monitor is a tool used to diagnose the messages flowing across the link. This is only useful for someone experienced with the message formats and protocols. These commands apply to CSLs or AMLs on ESDI cards and AMLs on MSDL cards.

DIS MSGI x	Disable output of incoming layer seven messages on AML x
DIS MSGO x	Disable output of outgoing layer seven messages on AML x
DIS PACI x	Disable output of incoming layer two messages on AML x
DIS PACO x	Disable output of outgoing layer two messages on AML x
DSIM MSGI <link#>	Disable inclusive incoming message monitoring
DSIM MSGO <link#>	Disable inclusive outgoing message monitoring
DSIT MSGI <link#><l><s><c><u>	Disable inclusive TN incoming message monitoring
DSIT MSGO <link#><l><s><c><u>	Disable inclusive TN outgoing message monitoring
DSXM MSGI <link#>	Disable all input message monitoring exclusions by the ENXM command.
DSXM MSGO <link#>	Disable all output message monitoring exclusions by the ENXM command.
DSXP MSGI <link#><pri><pri>...	Disable monitoring of exclusive priorities on incoming messages
DSXP MSGO <link#><pri><pri>...	Disable monitoring of exclusive priorities on outgoing messages
DSXT MSGI <link#><l><s><c><u>	Disable exclusive TN incoming message monitoring
DSXT MSGO <link#><l><s><c><u>	Disable exclusive TN outgoing message monitoring
ENIM MSGI <link#><msg1><msg2>...	Enable inclusive message monitoring of only those specified incoming messages
ENIM MSGO <link#><msg1><msg2>...	Enable inclusive message monitoring of only those specified outgoing messages

ENIT MSGI <link#><l><s><c><u>	Enable inclusive monitoring of incoming messages with specified TN
ENIT MSGO <link#><l><s><c><u>	Enable inclusive monitoring of outgoing messages with specified TN
ENL MSGI x	Enable output of incoming layer seven messages on AML x
ENL MSGO x	Enable output of outgoing layer seven messages on AML x
ENL PACI x	Enable output of incoming layer two messages on AML x
ENL PACO x	Enable output of incoming layer two messages on AML x
ENXM MSGI <link#><msg1><msg2>...	Enable message monitoring excluding those specified incoming messages
ENXM MSGO <link#><msg1><msg2>...	Enable message monitoring excluding those specified outgoing messages
ENXP MSGI <link#><pri><pri>...	Enable incoming message monitoring excluding messages with specified priorities
ENXP MSGO <link#><pri><pri>...	Enable outgoing message monitoring excluding messages with specified priorities
ENXT MSGI <link#><l><s><c><u>	Enable message monitoring excluding incoming messages with specified TN
ENXT MSGO <link#><l><s><c><u>	Enable input/output message monitoring excluding outgoing messages with specified TN
FLSH	Disable monitor and flash buffers
STAT MON (x)	Get status of one or all message monitors

Auxiliary Processor Link (APL) commands

The following commands are used to enable, disable, test and check the status of an APL link.

DIS APL x	Put software AUX link x in maintenance mode
DIS ISDI x	Disable hardware AUX link SDI x

ENL APL x	Put software AUX link x in non-maintenance mode
ENL ISDI x	Enable AUX link SDI x
STAT APL x	Display status of AUX link x
STAT DSP LNK x	Get status of all Displays on link x
STAT ISDI x	Get status of hardware AUX link SDI x

APL monitor commands

The APL monitor is a tool used to diagnose the messages flowing across the link. This is only useful for someone experienced with the message formats and protocols.

DIS PPRT x	Disable packet message print option on link x
DIS UPRT x	Disable unpacket message print on AUX link x
ENL PPRT x	Enable packet message print option on link x
ENL UPRT x	Enable unpacked message print on link x
ENLX MSGI x p	Output incoming priority p messages from link x
ENLX MSGO x p	Output outgoing priority p messages from link x
STAT CNFG	Get status of link monitor/simulator configuration
STAT CSDI x	Get status of SDI port x
STAT DSP LNK x	Get status of all Displays on link x

D-channel Expansion commands

Command	System Response	Description
DIS MSDL n all	GROUP	Disable the given MSDL card. All the configured ports should be in the disable state, otherwise the MSDL card can not be disabled.
DIS MSDL n ALL	GROUP	Disable all ports of the MSDL card, and then disable the MSDL card.

Command	System Response	Description
DIS MSDL n AUDM		
	GROUP	Disable the msdl auditing for the MSDL card.
DIS MSDL n DBG		
	GROUP	Disable the debugger option for the MSDL card.
DIS MSDL n FCTL		
	GROUP	Disable the flow control for the MSDL card.
DIS MSDL n MSGI		
	GROUP	Disable the incoming message monitor option for the MSDL card.
DIS MSDL n MSGO		
	GROUP	Disable the outgoing message monitor option for the MSDL card.
ENL MSDL n	GROUP	Enable the given MSDL card.
ENL MSDL n all	GROUP	Enable MSDL card n and all configured ports.
ENL MSDL n AUDM		
	GROUP	Enable the msdl auditing for the MSDL card.
ENL MSDL n DBG		
	GROUP	Enable the debugger option for the MSDL card.
ENL MSDL n FCTL		
	GROUP	Enable flow control for the MSDL card.
ENL MSDL n FDL		
	GROUP	Force download all the required Loadware to the MSDL card and enable the MSDL card.
ENL MSDL n MSGO		
	GROUP	Enable the outgoing message monitor option for the MSDL card.
ENL MSDL n MSGI		

Command	System Response	Description
	GROUP	Enable the incoming message monitor option for the MSDL card.
RST MSDL n	GROUP	This command causes a power-on reset on the MSDL card.
SLFT MSDL n	GROUP	Power-on reset on the MSDL card, followed by a complete set of self tests.
STAT MSDL	GROUP	Display status of all MSDL cards in the system.
STAT MSDL n	GROUP	Display status of the given MSDL card as known to the SL1.
STAT MSDL n full		
	GROUP	Display status of the given MSDL card as known to the SL1 and available in the shared RAM of the MSDL card.
STAT MSDL n MON		
	GROUP	Display the current message monitoring and debug option for the given MSDL card.

Intercept Computer Update (ICU) commands

DIS ICP x	Put ICP link x into maintenance mode
DSIC LSTI x	Disable printing of lost input messages on link x
DSIC LSTO x	Disable printing of lost output messages on link x
DSIC MSGI x	Disable printing of input messages on link x at input queue level
DSIC MSGO x	Disable printing of output messages on link x at output queue level
DSIC PACI x	Disable printing of input messages on link x at input buffer level
DSIC PACO x	Disable printing of output messages on link x at output buffer level
ENIC LSTI x	Enable printing of lost input messages on link x
ENIC LSTO x	Enable printing of lost output messages on link x
ENIC MSGI x	Enable printing of messages on link x at input queue level
ENIC MSGO x	Enable printing of messages on link x at output queue level

ENIC PACI x	Enable printing of input messages on link x at input buffer level
ENIC PACO x	Enable printing of output messages on link x at output buffer level
ENL ICP x	Enable ICP link x
ICP LINK xx	Set up ICP link x to be used in the ICP message
ICP DN xxxx	Set up ICP DN xxxx to be used in the ICP message
ICP IPN xx	Set up IPN number xx to be used in the ICP message
ICP RSN x	Set up the intercept transfer reason x to be used in the ICP message
ICP ADD xxxx	Set up additional information xxxx to be used in the ICP message
ICP CLR	Clear previous ICP message set up without sending it
ICP SEND xx yy	Send the defined ICP message number xx, yy times
ICPM	Access ICP maintenance commands
PSWD	Enter password to use ICP maintenance commands
STAT ICP (x)	Display software status of one or all ICP links

ISDN BRI monitor commands

These commands are used to monitor input/output messages to the MISP, and SILC/UILC. This is only useful for someone experienced with the message formats and protocols. A password is required for DGB and MON options. The SETM TNx, RSET TNx and RSET ALL commands are also available for digital telephones.

Caution: Use of the SETM MISP loop MON commands may use all system printing registers and cause an initialization.

RSET ALL	Reset (turn off) printing of messages for all terminal numbers associated with TN0-TN6.
RSET BRIM	Stop printing of messages on SILC/UILC, MISP or digital line card.
RSET MISP x AMO	Stop printing of audit messages on MISP specified.
RSET MISP x DGB	Exit MISP debug.
RSET MISP x MNT	Stop printing status messages on MISP specified.
RSET MISP x MON	Stop printing input/output messages on MISP specified.

RSET TNx	Stop printing of messages for terminal number associated with TNx. TNx is associated with the terminal number by the SETM TNx command.
SETM BRIM xxxx	Set printing of selected message types for MISP, SILC/UILC or digital line cards.
SETM MISP x AMO	Set printing of audit messages on MISP specified. The SETM TNx command must have been issued before issuing this command.
SETM MISP x DBG	Set debug option for the MISP specified. DISABLE MISP prior to issuing this command, re-enable MISP after command issued.
SETM MISP x MNT	Set printing of maintenance messages for the MISP specified.
SETM MISP x MON	Set printing of input/output messages for the MISP specified.
SETM TNx l s c u, dsl	Set printing messages on a unit
SETM TNx l s c u, 31	Set printing messages on a digital line card unit (u) or ISDN BRI line card (31)
SETM TNx y	Set printing of messages for specified digital line card unit or ISDN BRI line card.

Multipurpose Serial Data Link (MSDL) commands

The MSDL commands are listed below, x is the MSDL device number (defined by prompt DNUM in LD 17). These commands are also provided in Input/Output Diagnostic (LD 37) and D-channel Diagnostic (LD 96).

DIS MSDL x (ALL)	Disable MSDL device x
ENL MSDL x (ALL, FDL)	Enable MSDL device x
RST MSDL x	Reset MSDL device x
SLFT MSDL x	Invoke self-test for MSDL device x
STAT MSDL (x [FULL])	Get MSDL status

Single Terminal Access (STA) commands

Single Terminal Access (STA) is an application available on the MSDL card. The STA application reduces the number of physical devices used to administer and maintain the system

and its auxiliary processors. Refer to *Avaya System Management Reference, NN43001-600* for complete details.

DIS STA x	Disable the STA application
ENL STA x (FDL)	Enable STA application
MAP STA x	Get information relating to the STA application
STAT STA x	Get status of STA application

Voice Mailbox Administration (VMBA) commands

Voice Mailbox Administration (VMBA) allows for Integrated Voice Mailbox Administration when using Meridian Mail. Refer to the *Avaya Features and Services, NN43001-106* for complete details.

DIS VMBA <vsid>	Disable the Voice Mailbox Administration application
DIS VMBA <vsid> AUDT	Disable the mailbox database audit
DIS VMBA <vsid> UPLD	Disable the mailbox database upload
ENL VMBA <vsid>	Enable the Voice Mailbox Administration application
ENL VMBA <vsid> AUDT	Enable the mailbox database audit
ENL VMBA <vsid> UPLD	Enable the mailbox database upload
STAT VMBA <vsid>	Get the status for the Voice Mailbox Administration application
STAT VMBA <vsid> AUDT	Get the status for the Voice Mailbox database audit
STAT VMBA <vsid> UPLD	Get the status for the Voice Mailbox database upload

Alphabetical list of commands

Command	Description	Pack/Rel
CMIN	Clears minor alarm for all customers.	basic-1
CMIN ALL	Clears minor alarm for all customers.	basic-1

Command	Description	Pack/Rel
DACR ALL x	Release ALL devices on Link x	
DACR AGT l s c u	Release Agent	
DACR RTE x y	Release Route x for Customer y	
DIS AML x	Disable AML x. Whenever the third parameter (LYR2, LYR7, etc.) is not typed, the overlay defaults the third parameter of the DIS command to LYR2. Therefore, this command is equivalent to DIS AML x LYR2. Refer to DIS AML x LYR2 command definition, for more information.	msdl-18
DIS AML x AUTO	Disable AUTO recovery on AML x (MSDL only). This command is not available for an ESDI AML.	msdl-18
DIS AML x LYR2	Disable layer two on AML x. MSDL Requirement: The MSDL card must be enabled. The AML link state can be any state other than the disabled state, and should not be in the process of self-test. Example: ENL MSDL x followed by ENL AML x LYR2 must have been executed at an earlier time. MSDL Action: The AML link state is changed to the disable state. The MSDL port on which the AML is configured is disabled. ESDI: The ESDI port is disabled. The port must be idle.	msdl-18
DIS AML x LYR7	Disable layer seven on AML x. The MSDL or ESDI card must be enabled. The AML layer two must be enabled and established, and AML layer seven must also be enabled. Example: ENL MSDL x followed by ENL AML x LYR2 followed by EST AML x followed by ENL AML x LYR7 must have been executed at an earlier time. Action: A request to disable the AML layer seven is issued. SL-1 will stop sending polling messages to the far-end.	msdl-18
DIS AML x MDL	Disable MDL error reporting on AML x (MSDL only). MSDL Requirement: The MSDL card must be enabled. The AML layer two must be enabled. Example: ENL MSDL x followed by ENL AML x LYR2 must have been executed at an earlier time. MSDL Action: The MSDL AML loadware command to disable the debug monitor is sent to the MSDL card. This command is not available for ESDI AML.	msdl-18

Command	Description	Pack/Rel
DIS AML x MON	Disable monitor on AML x (MSDL only). MSDL Requirement: The MSDL card must be enabled. The AML layer two must be enabled. Example: ENL MSDL x followed by ENL AML x LYR2 must have been executed at an earlier time. MSDL Action: The MSDL AML loadware command to disable the debug monitor is sent to the MSDL card. This command is not available for ESDI AML.	msdl-18
DIS APL x	Put software AUX link x in maintenance mode.	apl-1
DIS ELAN TEST	Disable the ELAN subnet (server task)	nxcc-22
DIS ELAN x TEST	Disable ELAN subnet link number x (client task) **Note:** This command will disable the client task when the server task is disabled.	nxcc-22
DIS HSL	Disable the high-speed link.	lnk-2
DIS IALM <vsid>	Disable the integrated alarms application on the specified VAS. A VAS011 message is printed indicating the application has been disabled.	ialm-21
DIS ICP x	Put ICP link x into maintenance mode.	icp-5
DIS ISDI x	Disable hardware AUX link SDI x.	apl-1
DIS MON	Disable the monitor-bit of high-speed link data.	apl-1
DIS MSDL n all	Disable the given MSDL card. All the configured ports should be in the disable state, otherwise the MSDL card can not be disabled.	basic-25
DIS MSDL n ALL	Disable all ports of the MSDL card, and then disable the MSDL card.	basic-25
DIS MSDL x (ALL)	Disable MSDL device. When entered without the optional parameter, the disable MSDL command attempts to disable the MSDL card. Disabling the card via this command is permitted from either the Enabled (ENBL) state or the System Disabled (SYS DSBL) state.	msdl-18

Command	Description	Pack/Rel
	When attempted on an MSDL that does not have any ports enabled, this command will succeed. The only exception to this is when the disable card message needs to be sent to the card, and there is no buffer currently available for building the message (MSDL015 is output to the TTY). In this unusual situation, attempting the command again will most likely result in success. Application Overlays are not erased when the MSDL is disabled. If there are any ports that are still running in the MSDL card, the 'ALL' option must be used to force disable the active ports. As an alternative to this command, the craftsperson can use the commands provided by the applications to disable the ports (D-channels or AML) individually, and then use the 'DIS MSDL x' command. The command 'DIS MSDL x ALL' is not allowed if the active TTY (the terminal from which the command was entered) is supported on the MSDL card in question. Software disable the logical channel prior to disabling the physical DNUM port.	
DIS MSDL n AUDM		basic-25
	Disable the msdl auditing for the MSDL card.	
DIS MSDL n DBG	Disable the debugger option for the MSDL card.	basic-25
DIS MSDL n FCTL		basic-25
	Disable the flow control for the MSDL card.	
DIS MSDL n MSGI		basic-25
	Disable the outgoing message monitor option for the MSDL card.	
DIS MSGI x	Disable printing of messages on link x at input queue level. Disable output of incoming layer seven messages on AML x.	csl-8
DIS MSGO x	Disable printing of messages on link x at output queue level. Disable output of outgoing layer seven messages on AML x.	csl-8
DIS PACI x	Disable printing of input messages on link x at input buffer level. (disable output of incoming layer two messages on AML x)	csl-8

Command	Description	Pack/Rel
DIS PACO x	Disable printing of output messages on link x at output buffer level. (disable output of outgoing layer two messages on AML x)	csl-8
DIS PPRT x	Disable packet message print option on link x.	apl-1
DIS PRNT	Disable the print-bit of high-speed link data.	apl-1
DIS SDI HIGH	Disable the SDI port for high-speed link.	lnk-2
DIS SDI LOW	Disable the SDI port for low-speed link.	lnk-2
DIS STA x	Disable the STA application. This command disables the application, the administration port, and any other additional ports. The associated ports must be disabled before using this command. x = the logical ID number identifying the STA application.	sta-19
DIS TMDI l s c u (ALL)	Disable TMDI card.	basic-5.00
DIS UPRT x	Disable unpacket message print on AUX link x.	apl-1
DIS VMBA <vsid>	Disable the Voice Mailbox Administration application. This command is used to disable the Voice Mailbox Application. Enter the command in the following format: **DIS VMBA <vsid> <NNNN>** Where: • **vsid** = The VAS ID number associated with VMBA. • **NNNN** = AUDT or UPLD for the database audit or upload. AUDT and UPLD are optional entries. The VAS ID must be entered. The Voice Mailbox audit and upload functions are aborted when the application is disabled. Be sure to get the status of those functions before disabling the application.	vmba-19
DIS VMBA <vsid> AUDT		vmba-19

Command	Description	Pack/Rel
	Disable the mailbox database audit. This command aborts the audit function whether it was invoked manually or automatically.	
DIS VMBA <vsid> UPLD		vmba-19
	Disable the mailbox database upload. This command aborts the audit function whether it was invoked manually or automatically.	
DSIC LSTI x	Disable printing of lost input messages on link x.	icp-5
DSIC LSTO x	Disable printing of lost output messages on link x.	icp-5
DSIC MSGI x	Disable printing of input messages on link x at input queue level.	icp-5
DSIC MSGO x	Disable printing of output messages on link x at output queue level.	icp-5
DSIC PACI x	Disable printing of input messages on link x at input buffer level.	icp-5
DSIC PACO x	Disable printing of output messages on link x at output buffer level.	icp-5
DSIM MSGI <link#>		nxcc-22
	Disable inclusive incoming message monitoring	
DSIM MSGO <link#>		nxcc-22
	Disable inclusive outgoing message monitoring	
DSIT MSGI <link#><l><s><c><u>		nxcc-22
	Disable inclusive TN incoming message monitoring	
DSIT MSGO <link#><l><s><c><u>		nxcc-22
	Disable inclusive TN outgoing message monitoring	
DSXM MSGI <link#>		ncxx-22
	Disable all input message monitoring exclusions by the ENXM command.	
DSXM MSGO <link#>		ncxx-22

Command	Description	Pack/Rel
	Disable all output message monitoring exclusions by the ENXM command.	
DSXP MSGI <link#><pri><pri>...		nxcc-22
	Disable monitoring of exclusive priorities on incoming messages	
DSXP MSGO <link#><pri><pri>...		nxcc-22
	Disable monitoring of exclusive priorities on outgoing messages	
DSXT MSGI <link#><l><s><c><u>		nxcc-22
	Disable exclusive TN incoming message monitoring	
DSXT MSGO <link#><l><s><c><u>		nxcc-22
	Disable exclusive TN outgoing message monitoring	
ENIC LSTI x	Enable printing of lost input messages on link x.	icp-5
ENIC LSTO x	Enable printing of lost output messages on link x.	icp-5
ENIC MSGI x	Enable printing of messages on link x at input queue level.	icp-5
ENIC MSGO x	Enable printing of messages on link x at output queue level.	icp-5
ENIC PACI x	Enable printing of input messages on link x at input buffer level.	icp-5
ENIC PACO x	Enable printing of output messages on link x at output buffer level.	icp-5
ENIM MSGI <link#><msg1><msg2>...		nxcc-22
	Enable inclusive input/output message monitoring of only those specified incoming messages	
ENIM MSGO <link#><msg1><msg2>...		nxcc-22
	Enable inclusive input/output message monitoring of only those specified outgoing messages	
ENIT MSGI <link#><l><s><c><u>		nxcc-22

Command	Description	Pack/Rel
	Enable inclusive input/output monitoring of incoming messages with specified TN	
ENIT MSGO <link#><l><s><c><u>		nxcc-22
	Enable inclusive input/output monitoring of outgoing messages with specified TN	
ENL AML x	Enable AML x. For MSDL: If AUTO recovery is off, then this command is the same as the ENL AML x LYR2 command. If AUTO recovery is on, an attempt is made to establish the link (layer two) and the application (layer seven). For ESDI: This is the same as the ENL AML x LYR2 command.	esdi/ msdl-18
ENL AML x ACMS		esdi-18
	Enable automatic set-up on AML x (ESDI only). This command is valid only for ESDI AML and is not available on the MSDL AML.	
ENL AML x AUTO		msdl-18
	Enable AUTO recovery on AML x (MSDL only). This command is not available for ESDI AML links.	
ENL AML x FDL	Force download loadware to the MSDL card and enable AML x. MSDL Requirement: The MSDL card must be enabled. The AML link state must be in the disable state. All other MSDL AML links configured on the same MSDL card must be in the disable state. Example: ENL MSDL x must have been executed at an earlier time. MSDL Action: The MSDL AML loadware is downloaded to the MSDL card. While download is in progress a series of dots are output. Once the command is executed successfully the ENL AML x LYR2 command is executed automatically.	msdl-18
ENL AML x LYR2	Enable layer two on AML x. MSDL Requirement: The MSDL card must be enabled. The AML link state must be in the disable state. Example: ENL MSDL x must have been executed at an earlier time. MSDL Action: The AML link state is changed to the release state. The MSDL port on which the AML is configured is enabled. If the ENL AML x command is executed successfully, and MSDL AML auto recovery	msdl-18

Command	Description	Pack/Rel
	is in the enable state, then the EST AML x is issued automatically. ESDI: The ESDI port is enabled. The ESDI card must first be disabled.	
ENL AML x LYR7	Enable layer seven on AML x. MSDL Requirement: The MSDL card must be enabled. The AML link should not be in the simulation mode. The AML layer two must be enabled and established, and AML layer seven must be disabled. Example: ENL MSDL x followed by ENL AML x LYR2 followed by EST AML x must have been executed at an earlier time. MSDL Action: A request to enable the AML layer seven is issued. Polling messages are sent to the far end. ESDI: Layer seven is enabled for the ESDI AML. The ENL AML x (LYR2) command must be completed successfully first.	msdl-18
ENL AML x MDL	Enable MDL error reporting on AML x (MSDL only). MSDL Requirement: The MSDL card must be enabled. The AML layer two must be enabled. Example: ENL MSDL x followed by ENL AML x LYR2 must have been executed at an earlier time. MSDL Action: The MSDL AML loadware command to enable the MDL error reporting is sent to the MSDL card. This command is not available for ESDI AML links.	msdl-18
ENL AML x MON	Enable monitor on AML x (MSDL only). MSDL Requirement: The MSDL card must be enabled. The AML layer two must be enabled. Example: ENL MSDL x followed by ENL AML x LYR2 must have been executed at an earlier time. MSDL Action: The MSDL AML loadware command to enable the debug monitor is sent to the MSDL card This command is not available for ESDI AML links.	msdl-18
ENL APL x	Put software AUX link x in non-maintenance mode.	apl-1
ENL ELAN	Enable ELAN server task When the application establishes connection to a Meridian 1 via this ELAN subnet, a client process will be spawned for this application. The APP_IP_ID (Port ID and IP address) of each connection will be passed into the Meridian 1.	nxcc-22

Command	Description	Pack/Rel
ENL HSL	Enable the high-speed link. When enabling a high-speed link, the craftsperson must log out of the TTY to receive a message from the system which confirms that the high-speed link (HSL) has been enabled.	lnk-2
ENL IALM <vsid>	Enable the integrated alarms application on the specified VAS. A VAS011 message is printed if the application is successfully enabled and a VAS012 if it is not.	ialm-21
ENL ICP x	Enable ICP link x.	icp-5
ENL ISDI x	Enable AUX link SDI x.	apl-1
ENL MON	Print software information at maintenance TTY. This command causes software information being sent to the auxiliary processor to be printed at the TTY. This information would include counts of Cumulative Negative Acknowledgments (NAKs), time-outs and many other control characteristics of the link. Use this command only when the ACD is handling light traffic. Otherwise, the TTY will be overloaded from the high volume of messages.	apl-1
ENL MSDL n	Enable the given MSDL card.	basic-25
ENL MSDL n all	Enable MSDL card n and all configured ports.	basic-25
ENL MSDL x (FDL, ALL)	Enable MSDL card. When entered without any of the optional parameters, the enable MSDL command attempts to enable the MSDL card. Enabling the card via this command is only permitted if the card is currently in the Manually Disabled (MAN DSBL) state. The enable card succeeds if: 1. the card is resident in the shelf 2. it has passed all the self-tests 3. the MSDL base software has been downloaded and is responding If the MSDL base software and any configured application software has not been downloaded, or if the version of the software on the card is different from the version on the system disk, software download	msdl-18

Command	Description	Pack/Rel
	occurs. While download is in progress, a series of dots (".") are output. If the FDL (forced download) option is entered, the MSDL base software and all the configured applications will be downloaded regardless if the application already exists on the card. Following the download, the card will be enabled. If the ALL option is entered, the card will be enabled (provided the three conditions mentioned above are met), all the applications will be downloaded if necessary and then an attempt will be made to enable all the links/ports configured on the card. Additionally, the enable command with the ALL option can be entered when the card is already in the enabled state. This allows you to enable any disabled links/ports through one command. It is not possible to use both the ALL and the FDL options in the same command.	
ENL MSDL n AUDM		basic-25
	Enable the msdl auditing for the MSDL card.	
ENL MSDL n DBG	Enable the debugger option for the MSDL card.	basic-25
ENL MSDL n FCTL		basic-25
	Enable flow control for the MSDL card.	
ENL MSDL n FDL	Force download all the required Loadware to the MSDL card and enable the MSDL card.	basic-25
ENL MSDL n MSGO		basic-25
	Enable the outgoing message monitor option for the MSDL card.	
ENL MSDL n MSGI		basic-25
	Enable the incoming message monitor option for the MSDL card.	
ENL MSGI x	Print incoming messages from link x. Enable output of incoming layer seven messages on AML x. This command allows printing of all incoming message received over link x on the maintenance output device. The SSD signaling messages and the program input are not printed. This is typically used to check the validity of incoming messages for the different queues.	csl-8

Command	Description	Pack/Rel
ENL MSGO x	Print outgoing messages from link x. Enable output of outgoing layer seven messages on AML x. This command allows printing for all outgoing messages over link x on the maintenance output device. This is typically used to check the validity of outgoing messages sent from the application layer to the output queue.	csl-8
ENL PACI x	Print incoming ESDI messages from link x. Enable output of incoming layer two messages on AML x. When enabled, all incoming messages received on link x to the ESDI are printed on the maintenance TTY, including SSD signaling messages. Typically this is used to check the correctness of the incoming messages as received from the ESDI in the data block format.	csl-8
ENL PACO x	Print outgoing ESDI messages from link x. Enable output of incoming layer two messages on AML x. When enabled, all outgoing messages are sent through link x to the ESDI and are printed on the maintenance TTY. The message will be printed in the data block format required by the ESDI.	csl-8
ENL PPRT x	Enable packet message print option on link x. Printouts can be up to 7 lines in length and are of the form: • `APLO xxx y xxx. . . x` • `APLI xxx y xxx. . . x` Where: • `APLO` = the message is output from the system • `APLI` = the message is input to system from AUX • `xxx` = number of the APL link. • `y` = number from 0 to 6 indicating the printout line number of the message. This field is not used for ACK and NAK messages.	apl-1
ENL PRNT	Connect high-speed link to TTY. Disconnects the high-speed link from the AUX and connects it instead to an RS-232-C compatible TTY device. This disrupts communication between the system and the auxiliary processor. It enables ACD related messages (which would normally be sent to	apl-1

Command	Description	Pack/Rel
	the auxiliary processor) to be printed at the TTY connected to the high-speed link. Normal communication between the system and the auxiliary processor will not continue if the ENL PRNT command is inputted while the system and auxiliary processor are still connected. A different message format is used between the system and the auxiliary processor. This condition will cause the HSL to go down because the auxiliary processor cannot interpret this other message format.	
ENL SDI HIGH	Enable SDI port for high-speed link. When enabling a high-speed link, the craftsperson must log out of the TTY to receive a message from the system which confirms that the high-speed link (HSL) has been enabled.	lnk-2
ENL SDI LOW	Enable SDI port for low-speed link.	lnk-2
ENL STA x (FDL)	Enable STA application. The MSDL card must be enabled to implement this command, where: • x = the logical ID number identifying the STA application. • FDL = force download the application. If not invoked, the application is downloaded only when needed	sta-19
ENL TMDI l s c u	Enable TMDI card.	basic-5.00
ENL TMDI l s c u (FDL,ALL)	Enable TMDI card.	basic-5.00
ENL UPRT x	Enable unpacked message print on link x. Printouts are of the form: `APLMxxx aa b c zzzz. . . z` Where: • `APLMxxx` = indicates unpacked message over link xxx • `aa` = indicates the message length • `b` = indicates the application type • `c` = indicates the message type • `zzz` = these fields are the message body, depending on the application and message type	apl-1

Command	Description	Pack/Rel
ENL VMBA <vsid>	Enable the Voice Mailbox Administration application. Enter the command in the following format: ENL VMBA <vsid> <NNNN> ALL/xxxx Where: • vsid = The VAS ID number associated with VMBA. • NNNN = AUDT or UPLD for the mailbox database audit or upload functions. • ALL/xxxx = Enable NNNN for ALLDNs with Voice Mailboxes, or a specific DN (xxxx). NNNN and ALL/xxxx are optional entries. The VAS ID must be entered to initiate this command.	vmba-19
ENL VMBA <vsid> AUDT	Enable the mailbox database audit. Enter the command in the following format: ENL VMBA <vsid> AUDT ALL/xxxx The audit can be implemented for a specific Directory. Number by entering the DN following the audit command: ENL VMBA <vsid> AUDT xxxx The upload can also be enabled for all DNs eligible for a Voice Mailbox by entering ALL following the audit command: ENL VMBA <vsid> AUDT ALL	vmba-19
ENL VMBA <vsid> UPLD	Enable the mailbox database upload. Enter the command in the following format: ENL VMBA <vsid> UPLD ALL/xxxx The upload can be implemented for a specific Directory Number by entering the DN following the upload command: ENL VMBA <vsid> UPLD xxxx The audit can also be enabled for all DNs configured with Voice Mailboxes by entering ALL following the upload command: ENL VMBA <vsid> UPLD ALL	vmba-19
ENLX MSGI x p	Output incoming priority p messages from link x.	apl-1

Command	Description	Pack/Rel
	When enabled by the user, all incoming messages received on link x are output, excluding the messages with specified priorities, where "p" is the message priority, and where: • 1 = the system priority • 2 = signaling priority • 3 = call processing priority • 4 = administration priority	
ENLX MSGO x p	Output outgoing priority p messages from link x. When enabled by the user, all outgoing messages sent through link x are output, excluding the messages with specified priorities, where "p" is the message priority, and where: • 1 = the system priority • 2 = signaling priority • 3 = call processing priority • 4 = administration priority.	apl-1
EST AML x	Establish layer two on AML x. The layer two is established for the AML configured on the given MSDL port. The layer two is connected for the AML configured on the ESDI card. MSDL Requirement: The MSDL card must be enabled. The AML layer two must be enabled and released. Example: ENL MSDL x followed by ENL AML x LYR2 must have been executed at an earlier time. MSDL Action: The MSDL AML link state is changed into the established state. If EST AML x executes successfully, and provided that the MSDL AML AUTO recovery is enabled, next the ENL AML x LYR7 is executed automatically. ESDI: Layer two is connected for the ESDI AML. The port must be enabled first.	msdl-18
ENXM MSGI <link#><msg1><msg2>...		nxcc-22
	Enable message input/output monitoring excluding those specified incoming messages	
ENXM MSGO <link#><msg1><msg2>...		nxcc-22
	Enable message input/output monitoring excluding those specified outgoing messages	

Command	Description	Pack/Rel
ENXP MSGI <link#><pri><pri>...		nxcc-22
	Enable input/output incoming message monitoring excluding messages with specified priorities	
ENXP MSGO <link#><pri><pri>...		nxcc-22
	Enable input/output outgoing message monitoring excluding messages with specified priorities	
ENXT MSGI <link#><l><s><c><u>		nxcc-22
	Enable input/output message monitoring excluding incoming messages with specified TN	
ENXT MSGO <link#><l><s><c><u>		nxcc-22
	Enable input/output message monitoring excluding outgoing messages with specified TN	
FLSH	Disable monitor and flash buffers	nxcc-22
ICP ADD xxxx	Set up additional information xxxx to be used in the ICP message. Enter the time (hhmm) and date (mmdd).	icp-5
ICP CLR	Clear previous ICP message set up without sending it.	icp-5
ICP DN xxxx	Set up ICP DN xxxx to be used in the ICP message.	icp-5
ICP IPN xx	Set up IPN number xx to be used in the ICP message.	icp-5
ICP LINK xx	Set up ICP link xx to be used in the ICP message.	icp-5
ICP RSN x	Set up the intercept transfer reason x to be used in the ICP message.	icp-5
ICP SEND xx yy	Send the defined ICP message number xx, yy times. Where: • xx = number/type of ICP message (50-61 to the ICP link, 00-03 to the ICP module) • yy = number of times message is to be sent per time-slice (default = 1, maximum = 4)	icp-5

Command	Description	Pack/Rel
	The message is only cleared by entering the ICP CLR command or by changing the contents of the message.	
ICPM	Access ICP maintenance commands. Enter this command and the password (prompt PSWD) to use Intercept Computer Update (ICP) maintenance commands.	icp-5
MAP AML (x)	Get physical address and card name of one or all AMLs. This command outputs the card name and physical card address and ports for one or all AMLs. This information is also output with the STAT AML command. For example: • `MAP AML` • `AML: 05 ESDI: 04` • `AML: 12 MSDL:07 PORT:1`	msdl-18
MAP STA x	Get information relating to the STA application. This command displays the logical, physical, and port allocation information related to the STA application. If the ID number (x) is not specified, the information for all existing STAs is given.	sta-19
PSWD	Enter password to use ICP maintenance commands.	icp-5
RLS AML x	Release layer two on AML x. The layer two is released for the AML link configured on the given MSDL port. The layer two is disconnected for the AML configured on the ESDI card. MSDL Requirement: The MSDL card must be enabled. The AML layer two must be enabled and established. Example: ENL MSDL x followed by ENL AML x LYR2 followed by EST AML x must have been executed at an earlier time. MSDL Action: Prior to the execution of the RLS AML x, if the MSDL AML layer seven is enabled, the DIS AML x LYR7 is automatically executed. The MSDL AML state is changed to the release state. ESDI: The layer two is disconnected for the ESDI AML port. The port must be in the connected and idle state first.	msdl-18
RSET ALL	Stop printing all messages on a line card.	arie/ bri-14

Command	Description	Pack/Rel
RSET BRIM	Stop printing of messages on SILC/UILC, MISP or digital line card.	bri/ arie-18
RSET IFx 1 PDL2 1		mph-19
	Stop printing SAPI 16 interface messages.	
RSET IFx 1 PDNI n		mph-19
	Stop printing network interface messages.	
RSET IFx l s c u BCH x		mph-19
	Stop printing B-channel terminal interface messages.	
RSET IFx l s c u DCHx		mph-19
	Stop printing D-channel terminal interface messages.	
RSET IMSG l s c dsl		
	Disable monitoring on incoming	
RSET MISP x AMO		bri-18
	Stop printing of audit messages on MISP specified. Where: x = loop for non-Small System and card for Small System.	
RSET MISP x DGB		bri-18
	Exit MISP debug. Where: x = loop for non-Small System and card for Small System.	
	Where: x = loop 0-254 System with Fibre Network Fabric	fnf-25
RSET MISP loop MNT		bri-18
	Stop printing of status messages on MISP specified. Where: x = loop for non-Small System and card for Small System.	
	Where: x = loop 0-254 System with Fibre Network Fabric	fnf-25
RSET MISP x MON		bri-18
	Stop printing of input/output messages on MISP specified. Where: x = loop for non-Small System and card for Small System.	
	Where: x = loop 0-254 System with Fibre Network Fabric	fnf-25

Command	Description	Pack/Rel
RSET MPHM	Stop all Meridian Packet Handler message monitoring.	mph-19
RST MSDL n	This command causes a power-on reset on the MSDL card.	basic-25
RSET OMSG l s c dsl	Disable monitoring on outgoing	
RST TMDI l s c u	Reset TMDI card	basic-5.00
RSET TNx	Stop printing messages on an ISDN BRI line card. Where: x = 0-6 (TN0-TN6).	bri-18
RST MSDL x	Reset MSDL card. This command causes a power-on reset on the MSDL, followed by a series of short self-tests. Resetting the card via this command is only permitted if the card is in the Manually Disabled (MAN DSBL) state.	msdl-18
SET IMSG l s c dsl MON x	Set monitor on incoming msg	
SET OMSG l s c dsl MON x	Set monitor on outgoing msg	
SETM BRIM xxxx	Set printing of messages on SILC/UILC, MISP, or digital line card. This command is used to select various message types for printing on a given TN (defined by SETM TNx commands). The value of xxxx is a HEX word which determines the message types.	bri-18

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
			x							x	x	x	x	x	x

- Bit 0 = Input SSD message from BRI line cards.
- Bit 1 = Output SSD message to BRI line cards.
- Bit 2 = Input expedited (high priority) message from BRIL application on MISP.
- Bit 3 = Output expedited (high priority) message from BRIL application on MISP.

Command	Description	Pack/Rel
	• Bit 4 = Input ring message from BRIL application on MISP. • Bit 5 = Output ring message from BRIL application on MISP • Bit 12 = Call processing error message. • All other Bits are for future use. Note that the SETM TNx command must have been issued before issuing this command. EXAMPLE: To print input SSD and expedited messages: SETM BRIM 0005 (i.e., 0000000000000101) To print input and output expedited messages: SETM BRIM 000C (i.e., 0000000000001100)	
SETM IFx 1 PDL2 1		mph-19
	Set printing of SAPI 16 interface messages.	
SETM IFx 1 PDNI n		mph-19
	Set printing of network interface messages.	
SETM IFx l s c u BCHx		mph-19
	Set printing of B-channel terminal interface messages.	
SETM IFx l s c u DCHx		mph-19
	Set printing of D-channel terminal interface messages.	
SETM MISP x AMO		bri-18
	Set printing of audit messages on MISP specified. Where: x = loop for non-Small Systems and non-CS 1000S and card for Small Systems and CS 1000S. These messages are sent from the MISP handler to the MISP basecode. This command is used to turn these messages back on once they have been turned off because: • debug or monitor (MON) mode is enabled • RSET x AMO command has been issued Where: x = loop 0-254 System with Fibre Network Fabric	fnf-25

Command	Description	Pack/Rel
SETM MISP x DBG		bri-18
	Set debug option on MISP specified, where: x = loop.The card must be disabled first. The debug option has the following effect when the MISP is enabled: • turns off the sanity timer • stops interface handler audit messages • no timestamp messages are sent to the MISP card This command requires a password. The "dot" prompt indicates debug mode is turned on.	
SETM MISP x MNT		bri-18
	Set printing of status messages on MISP specified, where: • x = loop for Large Systems and CS 1000E • x = card for Small Systems and CS 1000S These messages indicate: • error indication messages from the MISP • state of L1 on SILC/UILC and L2/L3 on MISP This option setting is lost during an initialization.	
SETM MISP x MON		bri-18
	Set printing of input/output messages on MISP card. Where: x = loop for non-Small System and card for Small System. Both the expedited and ring input/output messages are printed. This command also sets the debug option and requires a password. This command turns on all input/output messages. This may use up all system print registers and may cause system initialization. Therefore use this command with caution. The debug option is turned off by a system initialization. Restarting debug will also restart the input/output monitoring. DISABLE MISP prior to issuing this command, re-enable MISP after command issued.	
SETM MPHM xxxx		mph-19
	Set printing of Meridian Packet Handler messages. Where: xxxx = the MPHs to be monitored	

Command	Description	Pack/Rel
SETM TNx l s c u, 31	Set printing messages on a digital line card unit (u) or ISDN BRI line card (31). This command is used in conjunction with the SETM BRIM command. The value x is a tag number (0-6). For ISDN BRI line cards, you must enter "l s c 31" for the address.	arie/ bri-14
SETM TNx l s c u, dsl	Set printing messages on a unit. This command is used in conjunction with the SETM BRIM command. The value x is a tag number (0-6).	arie/ bri-14
SETM TNx y	Set printing messages on a digital line card unit or ISDN BRI line card. Where: x = tag number 0-6 (TN0-TN6) y = l s c u (loop, shelf, card, and unit) or l s c dsl (loop, shelf, card, and digital subscriber loop) for non-Small Systems and non-CS 1000S and c u (card, and unit) or c dsl (card, and digital subscriber loop) for Small Systems and CS 1000S. If u = 31 when a S/T (SILC) or U (UILC) Interface Line Card is specified for the y parameter, then messages for that line card are printed. This command must be issued before the SET BRIM command.	bri-18
SLFT AML x	Self-test on AML x. This command runs the local loop back test for MSDL AML, and the ESDI self-test for the ESDI AML. MSDL Requirement: The MSDL card must be enabled. The AML layer two must be disabled. Example: ENL MSDL x must have been executed at an earlier time. MSDL Action: The MSDL AML local loop back test is executed and upon completion of the test the MSDL AML port is set to the disable state.	msdl-18
SLFT MSDL x	Execute a self-test on MSDL card x. This command causes a power-on reset on the MSDL, which ill be followed by a complete set of self-tests. This command only executes self-tests if the card is in the Manually Disabled (MAN DSBL) state. If the self-tests pass, a message indicating this and card id is output. If the self-tests fail, a message is output describing which self-test failed. It is useful to note that the first test that fails will abort the self-test sequence, so this command only indicates one test failure, even if multiple tests might fail.	msdl-18

Command	Description	Pack/Rel
SLFT TMDI l s c u	Invoke self test	basic-5.00

STAT AML (x)	Get AML status.
	This command outputs the status of layer two and layer seven of one or all configured AMLs. The designation (DES) of the AML is output if it has been defined for the port in LD 17.
	Examples:
	`AML: 01 MSDL: 08 PORT: 00`
	`LYR2: DSBL AUTO: OFF LYR7: DOWN`
	`DES: MERIDIAN_MAIL`
	`AML: 04 ESDI: 10`
	`LYR2: EST AUTO: ON LYR7: ACTIVE`
	Where x = 47 (127)
		msdl-18

STAT APL x	Display status of AUX link x.	apl-1
STAT CNFG	Get status of link monitor/simulator configuration. Display link monitor/simulator configuration status. The system will respond according to the current configuration as follows: • `*NOT CONFG` - if system is not configured • `*CNFG INT/SIM CSLAPL x CSLSIM x` if the system is in internal maintenance mode; shows link numbers of CSLSIM and CSL application program • `*CNFG FLD CSL x` if the system is in field maintenance mode; shows CSL link number	csl-8
STAT CSDI x	Get status of SDI port x.	basic-1
STAT DSP LNK x	Get status of all Displays on link x.	apl-1
STAT ELAN [<x>]	Check status of a configured AML over Ethernet (ELAN subnet) link. Where <x> = a specific AML over Ethernet (ELAN subnet) link. If no AML over Ethernet link is specified, the statuses of all configured ELAN subnets are checked.	nxcc-22
STAT HSL	Get high-speed link status. Response can be either: `1. UP` `2. DOWN,` or `3. NOT READY`	lnk-2
STAT IALM <vsid>		ialm-21

Command	Description	Pack/Rel
	Print the status of the integrated alarms application on the specified VAS, where: • ACTIVE = active IALM application • INACTIVE = inactive IALM application • MANDIS = manually disabled IALM application (disabled in LD 48) • LINKOOS = inactive IALM application (because link to the AP is out of service)	
STAT ICP (x)	Display software status of one or all ICP links.	icp-5
STAT ISDI x	Get status of hardware AUX link SDI x.	apl-1

STAT MON (x)	Get status of one or all message monitors.
	The system will respond with the status. If all monitors are disabled, the response is:
	`MSGO DIS`
	`MSGI DIS`
	`PACO DIS`
	`PACI DIS`
	`X25I DIS`
	`X25O DIS`
	If the monitor function is enabled, for outgoing messages on two links, the response is: `MSGO ENL CSL x`
		csl-8

STAT MSDL (x (FULL))	Get MSDL status.
	This command outputs the status of MSDL cards. Without any optional parameters (no card number, etc.), the status of all MSDL cards in the system is output.
	When a card number alone is provided with the command, the status of the card is output along with additional information regarding the applications configured on the card.
	Specifically, for each D-channel or AML configured on the card, the application name, logical number and port status is output.
	For example:
	`MSDL x: ENL`
	`AML 11 DIS  PORT 1`
	`DCH 25 OPER PORT 2`
	`AML 03 OPER PORT 3`
		msdl-18

Command	Description	Pack/Rel

	For example:
	`MSDL x: ENL`
	`SDI 7 OVLD PORT 0`
	`AML 11 DIS PORT 1`
	`DCH 25 OPER PORT 2`
	`AML 03 OPER PORT 3`
	
	If the FULL option is entered along with the MSDL number, the system outputs all the information output for the 'STAT MSDL x' command along with the following additional information:
	• card ID
	• bootload firmware version
	• basecode version
	• basecode state
	• when the basecode was activated (if it is active)
	• each application version
	• each application state
	• when each the application was activated (if it is active)
	
	The card status is output on the first line and can be any one of the following:
	`MSDL x: ENBL` - card is enabled
	`MSDL x: MAN DSBL` - card disabled by the DIS MSDL command
	`MSDL x: SYS DSBL reason` - card has been disabled by the system
	
	The system disabled state may be due to any of the following:
	1. `SYS DSBL- NOT RESPONDING`
	• If the MSDL is in this state, the implication is that the system has attempted to communicate with the MSDL and was not successful. It is possible that the card is not present in the shelf. If it is present, then it is possible that the software on the card is unable to respond to messages from the system.
	• Action: Check to see if the card is properly inserted in its slot. If it is (and has been for more than a few minutes), then check the console output for MSDL or ERR messages and take the appropriate action for the error message.
		msdl-24

Command	Description	Pack/Rel

- It may be that the rotary switch setting on the MSDL card is not set properly. To keep the system from continuously attempting recovery of the MSDL, use the 'DIS MSDL x' command to put the card in the Manually Disabled (MAN DSBL) state.

2. SYS DSBL- SELF-TESTING

   - If the MSDL is in this state, self-tests are in progress.
   - Action: Wait for self-tests to complete and for the system to examine the results. Under normal circumstances, self-tests take less than one minute to complete. However, when an erasable EPROM on the card has been cleared, self-tests may take between five and six minutes to complete. Therefore, it is prudent not to take any action at this time.

3. SYS DSBL- SELF-TESTS PASSED

   - This is a transient state. A card in a transient state has successfully completed self-tests and the system either is about to begin downloading the MSDL base software, or has just completed downloading the MSDL base software and is about to attempt to enable the card.
   - Action: Wait for the system to begin the next step of recovery. If a more immediate recovery is desired, use the 'DIS MSDL x' command followed by the 'ENL MSDL x' command. This causes essentially the same recovery action to be taken. However, it may be faster (since it is being done as a result of input from the craftsperson).

4. SYS DSBL- SELF-TESTS FAILED

   - If the MSDL is in this state, self-tests have executed and failed on this card.
   - Action: Use the 'STAT MSDL x' command to determine reason for self-test failure. Disable the MSDL card using the 'DIS MSDL x' command, then use the 'SLFT MSDL x' command to execute the self-tests again.
   - If the self-tests pass, attempt to enable the card using the 'ENL MSDL x' command. If the card fails the self-tests again, record the results and replace the card.

Command	Description	Pack/Rel

5. SYS DSBL- SRAM TESTS FAILED

   - If the MSDL is in this state, self-tests have executed and passed, however when the system attempted to perform read/write tests to the shared RAM on the MSDL, it detected a failure.
   - Action: Same as for self-test failure. If the attempt to enable the card fails, record the results and replace the card.

6. SYS DSBL- OVERLOAD

   - The system has received too many messages from the MSDL. This is considered to be unacceptable, in that this much of a demand may interfere with other system functions.
   - Action: If the MSDL is left in this state, the system will attempt to bring the card back into service within a few minutes. If this is not desired, disable the card using the 'DIS MSDL x' command.
   - It is also advisable to identify a specific port or application that may be responsible for the overload. The identification can be made by disabling individual links/ports on the MSDL and letting the remaining links/ports operate normally.

7. SYS DSBL- RESET THRESHOLD

   - If the MSDL is in this state, the system has detected more than four resets within ten minutes. This is considered to be unacceptable, as a normally operating card should not reset so often.
   - It is possible that the card may be in this state due to a Fatal Error or Self-test failure from which no recovery was successful. (As the recovery from Fatal Errors and Self-test failures begins with resetting the card, repeated attempts at recovery may cause the reset threshold to be reached.)
   - Action: Disable the card using the 'DIS MSDL x' command and execute the 'SLFT MSDL x' command. If self-tests pass, attempt to enable the card using the 'ENL MSDL x' command. If the problem recurs, try force downloading the

Command	Description	Pack/Rel

software to the MSDL using the 'ENL MSDL x FDL' command.

- If the problem continues to recur and resets continue because of a repeated fatal error, attempt to isolate the problem by disabling all links/ports controlled by one application (e.g., all D-channels or all AMLs). If no manual intervention is taken by the craftsperson, the system will attempt to bring the card back into service beginning at midnight.

8. `SYS DSBL- FATAL ERROR`

   - If the MSDL is in this state, the card encountered a fatal condition from which it could not recover. In response to the 'STAT' command, the cause of the fatal error will be displayed.
   - If the 'STAT' command is not entered while the card is in this state, the MSDL302 message printed at the time of the state transition will indicate the cause of the fatal error.
   - Action: The system will attempt to bring the card back into service automatically. While the card is in this state, it is recommended that the craftsperson do nothing. If the system is unable to recover the card, the system disabled substate will be changed to indicate the reason recovery was not possible. The craftsperson should then take the recommended action for that new substate.

9. `SYS DSBL- NO RECOVERY ATTEMPTED UNTIL MIDNIGHT`

   - When this is output after the SYS DSBL message, the system has attempted to recover the card but has repeatedly failed. One example of this condition is when the background recovery mechanism has failed to download the MSDL Base Code five times in a row.
   - Action: Disable the card using the 'DIS MSDL x' command, test the card using the 'SLFT MSDL x' command, and if self-tests pass, enable the card using the 'ENL MSDL x' command.
   - If downloading of the MSDL Base Code is necessary, it will be attempted in response to

Command	Description	Pack/Rel
	the enable command. If no manual intervention is taken, the system will again attempt recovery beginning at midnight.	
STAT SDI HIGH	Get status of high-speed link port. The response can be either ENL (enabled) or DIS (disabled).	lnk-2
STAT SDI LOW	Get status of low-speed link port. The response can be either ENL (enabled) or DIS (disabled).	lnk-2
STAT STA x	Get status of STA application. When x (STA ID number) is specified, the STA state, port number, port type, port state, and system description are displayed. If x is not specified, and the application is enabled, the state and port information is given. If x is not specified, and the application is in any state other than enabled, only the STA status is given. No port or system information is displayed. Possible output follows: • Application state and Target state: `ENABLED, MANUAL DISABLE, SYSTEM DISABLE, AWAIT DISABLE, AWAIT APPL ENABLE, AWT CONF DOWNLOAD` • Port type: `ADM, SYS, TTY` • Port state: `NO SDI/STA, DISABLED, ENABLED, TESTING, KEYBOARD TST, AWAIT VT-200, DTR DOWN, AUTOBAUDING, AWT AUTOBAUD, ABD SCANNING, DEFAULT ABD, NO MODEM, IN SESSION, AWAIT ENABLE` System description is entered as part of the port configuration. For the additional port used to shadow the STA application, the system description is SHADOW TTY.	sta-19
STAT TMDI l s c u (FULL)	Get TMDI status	basic-5.00
STAT VMBA <vsid> [<NNNN>]		vmba-19
	Get the status for the Voice Mailbox Administration application, where:	

Command	Description	Pack/Rel
	• vsid = the VAS ID where the VMBA is configured • NNNN = VMBA audit or upload function, where: - AUDT = mailbox database audit - UPLD = mailbox database upload AUDT and UPLD are optional entries. The VAS ID must be entered. The status output is shown below: STAT VMBA <vsid> • VMBA <ACTIVE or INACTIVE> • AUDIT <ACTIVE or INACTIVE> • UPLOAD <ACTIVE or INACTIVE> STAT VMBA <vsid> AUDT AUDIT INACTIVE, or AUDIT ACTIVE Where: • n AUDITED • n MISMATCHES FOUND/CORRECTED • n ERRORS STAT VMBA <vsid> UPLD UPLOAD INACTIVE, or UPLOAD ACTIVE Where: • n UPLOADED • n DELETED • n ERRORS	
STAT VMBA <vsid> AUDT	Get the status for the Voice Mailbox Database audit. Enter the command in the following format. STAT VMBA <vsid> AUDT The status output is shown below: STAT VMBA <vsid> AUDT AUDIT INACTIVE, or AUDIT ACTIVE Where: • n AUDITED • n MISMATCHES FOUND/CORRECTED • n ERRORS	vmba-19

Command	Description	Pack/Rel

STAT VMBA <vsid> UPLD	Get the status for the Voice Mailbox Database upload.
	Enter the command in the following format.
	STAT VMBA <vsid> UPLD
	The status output is shown below:
	`STAT VMBA <vsid> UPLD`
	`UPLOAD INACTIVE,or UPLOAD ACTIVE`
	Where:
	• `n UPLOADED`
	• `n DELETED`
	• `n ERRORS`
		vmba-19

SWCH AML x y	Switch active (x) and standby (y) AML. This is AML switchover, where x is the active AML switching to standby and y is the standby AML to become active.	msdl-18
UPLD AML x TBL y	Upload parameter table 1 to 4 from AML x (MSDL only). The MSDL AML maintenance error log table, is uploaded from the MSDL card and is displayed on the TTY screen. The parameter tables are: • TBL1 = AML maintenance error log table • TBL2 = AML downloaded parameter table • TBL3 = AML protocol error log table • TBL4 = AML traffic table MSDL Requirement: The MSDL card must be enabled. The AML layer two must be enabled. Example: ENL MSDL x followed by ENL AML x LYR2 must have been executed at an earlier time. Action: MSDL AML table is uploaded and is displayed on the TTY screen. This command is not available for the ESDI card.	msdl-18

Chapter 22: LD 51: Intercept Computer Update

This program updates the system with the intercept service interface information that is stored. The program can be run manually or run in the midnight routine for all customers.

Basic commands

CUST ALL	Update all customers.
CUST c ...c	Update 1 to 5 customers (0-99).
END	Terminate the program.
UPD	Update the transfer information.

Alphabetical list of commands

Command	Description	Pack/Rel
CUST ALL	Update all customers.	icp-5
CUST c ...c	Update 1 to 5 customers (0-99). Repeat the command if more than 5 customers are to be updated.	icp-5
END	Terminate the program.	icp-5
UPD	Update the transfer information.	icp-5

Chapter 23: LD 54: Multifrequency Signaling Diagnostic

Multifrequency Compelled Signaling (MFC) or Multifrequency Signaling (MFE) provides a handshaking facility between the system and the Central Office or Public Exchange (CO/PE) or between other PBXs over network/Tie trunks.

The XMFC card on a superloop can be used for MFC or MFE. XMFC card has four units.

The MFD overlay program is used to diagnose, display or change the status of the MFC or MFE send/receive (S/R) cards.

The program resets all available MFC or MFE cards (for channels on AXMFC card) and performs loop back tests during the midnight routines. After every SYSLOAD or power-up, all available MFC or MFE cards are initialized.

The program can be loaded by the system after every power-up (or SYSLOAD), as part of the daily routines, or loaded manually to enter commands.

Hardware Initialization after SYSLOAD

After system power-up, every idle MFC or MFE card is initialized (self-tested). During this test the card is disabled (LED on faceplate ON) and the S/R card microprocessor executes sequential loop back tests on both channels.

On power-up SYSLOAD on XMFC, card performs self-test, LED blinks 3 times to indicate self-test pass:

- Cardlan polling message indicates that XMFC card has powered up.
- MSL-1 down loads the configuration (E0XXH)
- MSL-1 enables the card (C000H)
- Card performs self-test again. If self-test passes (8000H), then LED is OFF and card is enabled. If self-test fails (80XXH), LED is ON and card is disabled.

These tests entail looping the sender output of each card to the Receiver input. The sender transmits all thirty tone pairs (1 to 15 digits for both DOD/DID modes) with a default signal level of zero. Each time the receiver detects a tone pair, the microprocessor verifies the digit received. At the end of the test the microprocessor tries to send two test results (one for each channel) to the CPU.

The CPU cannot receive the results of the test because the card is disabled. A command to enable the card is issued and the microprocessor sends the test results to the CPU.

Loop around test during daily routines

This loop around test is conducted by the system during the midnight routines. The midnight test is identical to the test conducted after power-up except for the following points:

- the midnight test is conducted on one channel at a time for all available MFC or MFE cards
- the MFC or MFE S/R card remains enabled (LED on faceplate OFF)
- the midnight self-test can also be loaded manually by issuing a command on the specified channel

Loop around test by command

The loop around tests are performed by maintenance personnel on a specified channel of the MFC or MFE S/R card. There are two types of tests:

- one is identical to the midnight test which is conducted on the specific channel
- the second is conducted on a specific channel for a specified digit and signal level

LD 54 also performs the following functions:

- resets all idle MFC or MFE cards once a day during the midnight routines
- disables MFC or MFE card or channel. It enables MFC or MFE card or channel
- determines the status of MFC card or channel
- lists all disabled MFC or MFE channels
- handles other common overlay operations (such as clear alarms)

Note:
Use the DISL command to force-disable the MFC or MFE channel or card.

Note:
Use the DISI command in LD 32 to disable the card when idle.

Note:
No more than 50% of MFC channels can be disabled at one time as a result of system or manually initiated tests. However, this constraint does not apply using disable commands.

MFC/MFE error handler and counter

The MFC/MFE error handlers are resident programs that monitor the number of MFC or MFE signaling errors. A one-word error field in the MFC or MFE block is initialized to zero. The Error Handler program allows a maximum of 10 errors. After every successful use of the MFC or MFE channel, the error field will decrement by one, if it is not already at zero. After every failure of the MFC or MFE channel the error field will increment by one.

In Generic software, the Error Handler program generates only the ERR700 L S C U message. When an Error Handler code is output, the MFD Overlay must be loaded manually and the MFC or MFE channels tested.

Fibre Network Fabric

The Fibre Network Fabric extends and enhances the 5-group network architecture to 8 non-blocking (inter-group) Network groups, with a resulting expansion in network capacity to 8k timeslots available for Intergroup traffic. This is achieved by using OC-12 SONET rings, and adding additional network and IPE shelves, cards and cables and software changes to allow using the expanded network capacity. This expansion increases the number of available loops from 160 to 256. This applies to Multi Group systems only.

Basic commands

ATST l s c u	Invoke automatic loop around test for specified unit
CDSP	Clear maintenance display to 00 or blank
CMAJ	Clear major alarm and reset power fail transfer
CMIN	Clears minor alarm for all customers.
CMIN ALL	Clears minor alarm for all customers.
DISC l s c	Disable specified MFC or MFE card
DISU l s c u	Disable specified MFC or MFE channel
END	Stop further testing or cancel active command
ENLC l s c	Enable specified MFC or MFE card
ENLU l s c u	Enable specified MFC or MFE channel

MIDN 0	Reset all idle MFC or MFE cards
MIDN 1	Initialize all idle MFC or MFE cards
MTST l s c u d l	Invoke manual loop around test on unit with specified digit and level
STAT	List all disabled MFC channels in the system
STAT l s c (u)	Get status of specified MFC or MFE card or unit

Alphabetical list of commands

Command	Description	Pack/Rel
ATST l s c u	Invoke automatic loop around test for specified unit. Performs automatic loop around test on specified unit with default signal level of zero. All 30 tone pairs are tested and verified by the card microprocessor. Digits 1 to 15 signify Forward Signals 1 to 15 (DOD mode) and digits 16 to 30 signify Backward Signals 1 to 15 (DID mode). The response is OK when the unit passes test and is enabled. If the receiver sends no message within a predefined time period, an error message indicating time-out is printed. If the receiver indicates it has received a different signal than that sent, the failed signal, an error message and the TN are printed.	basic-1
CDSP	Clear maintenance display to 00 or blank.	basic-1
CMAJ	Clear major alarm, reset power fail transfer and clear power fault alarm.	basic-1
CMIN	Clears minor alarm for all customers.	alrm_filter-22
CMIN ALL	Clears minor alarm for all customers.	basic-1
DISC l s c	Disable specified MFC or MFE card. LED on card is ON when disabled.	basic-1
DISU l s c u	Disable specified MFC or MFE channel. When the other unit on the card is also in a disabled state in the software, a message is sent to disable the MFC or MFE card. LED on card is ON when disabled.	basic-1

Command	Description	Pack/Rel
END	Stop further testing or cancel active command.	basic-1
ENLC l s c	Enable specified MFC or MFE card. Response is `OK` . A message is sent to the MFC or MFE card to turn off the LED.	basic-1
ENLU l s c u	Enable specified MFC or MFE channel. Response is `OK` . A message is sent to the MFC or MFE card to turn off the LED.	basic-1
MIDN 0	Reset all idle MFC or MFE cards. Resets all idle MFC or MFE cards and performs loop around tests on all idle channels.	basic-1
MIDN 1	Initialize all idle MFC or MFE cards. Recommended after installation.	basic-1
MTST l s c u d l	Invoke manual loop around test on unit with specified digit and level. This command performs the manual loop around test on specified unit with specified digit and signal level. MFC-30 tone pairs are tested and verified by the system CPU. Digits 1 to 15 indicate forward signals 1 to 15 (DOD mode) and digits 16 to 30 indicate backward signals 1 to 15 (DID mode). MFE-15 tone pairs are tested and verified. Digits 1-15 represent Forward Signals 1-15 (DID mode). Digit 0 represents the control frequency. Table 14: MFC sender/transmit levels on page 265 presents MFC sender (transmit) levels. These levels are output by the MFC card and do not include any pads that may be put in by the trunk card.	basic-1

Table 14: MFC sender/transmit levels

Digit level	Level at S/R card	Digit level	Level at S/R card
0	8 dBm	8	4 dBm
1	11 dBm	9	5 dBm
2	12 dBm	10	6 dBm
3	13 dBm	11	7 dBm
4	14 dBm	12	9 dBm
5	15 dBm	13	10 dBm
6	16 dBm	14	spare (8) dBm

Digit level	Level at S/R card	Digit level	Level at S/R card
7	31 dBm	15	spare (8) dBm

	The MFE signal level 0 = -10.5 dBm level with skew -7.0 dBm control frequency level. Signal levels 1-7 are used for internal test purposes. The response is `OK` when the unit passes the test and is enabled. If the unit fails the test, the appropriate error message and the TN are printed.	
STAT	List all disabled MFC channels in the system.	basic-1
STAT l s c (u)	Get status of specified MFC or MFE card or unit. Status is one of: `IDLE, BUSY, MBSY, DSBL` or `UNEQ` for both channels.	basic-1

Chapter 24: LD 60: Digital Trunk Interface and Primary Rate Interface Diagnostic

The LD 60 diagnostic program can be run in midnight routines or loaded manually to enter commands.

On Small Systems and CS 1000S systems, LD 60 is used to maintain:

- NTAK20 Clock Controller
- NTAK09 1.5 Mb/s (DTI/PRI) Interface Card
- NTAK10 2.0 Mb/s (DTI) Interface Card
- NTAK79 2.0 Mb/s (PRI)
- NTRB21 TMDI
- NTAK50 2.0 Mb/s

This program is used to maintain the following on other systems:

- QPC471/775 Clock Controller
- QPC472 1.5 Mb/s Digital Trunk Interface (DTI)
- QPC536 2.0 Mb/s Digital Trunk Interface (DTI2)
- QPC720 or DDP2 Primary Rate Interface (PRI)
- NT8D72AA 2.0 Mb/s Primary Rate Interface (PRI)

Channel Timeslot Mapping

If a system loop is configured with a SYS-12, AXE-10 SWE, NUMERIS, SwissNet D-channel (SWISS), TCNZ, or EuroISDN, then the following message to explain the difference in timeslot to channel mapping between the system and the public network will be printed on loading the Overlay. The heading will differ according to the interface supported by the phase. Refer to Table 15: Channel Timeslot Mapping on page 268 for channel timeslot mapping.

Example Message:

M1/SL-1 — SYS-12

AXE-10 SWE

NUMERIS

SWISS

TCNZ

EuroISDN

Table 15: Channel Timeslot Mapping

Channel	M 1/SL-1	Network	Timeslot
B	1-15	1-15	1-15
B	16-30	17-31	17-31
D	31	16	16

Fibre Network Fabric

The Fibre Network Fabric extends and enhances the 5-group network architecture to 8 non-blocking (inter-group) Network groups, with a resulting expansion in network capacity to 8k timeslots available for Intergroup traffic. This is achieved by using OC-12 SONET rings, and adding additional network and IPE shelves, cards and cables and software changes to allow using the expanded network capacity. This expansion increases the number of available loops from 160 to 256. This applies to Multi Group systems only.

Basic commands

DTI/PRI commands

ATLP (0), 1	Disable (default) or enable midnight auto loop test
CDSP	Clear maintenance display to 00 or blank
CMIN	Clears minor alarm for all customers.
CMIN ALL	Clears minor alarm for all customers.
DISI loop	Disable loop when all channels are idle
DISL loop	Disable network and DTI/PRI cards of loop

DLBK loop	Disable remote loop back test per RLBK command
DLBK l ch	Disable remote loop back test per RLBK l ch command
DSCH l ch	Disable channel ch of loop
ENCH loop	Enable all channels on 2.0 Mb/s DTI/PRI
ENCH l ch	Enable channel ch of DTI/PRI loop
ENLL loop	Enable network and DTI/PRI cards of loop
LCNT (loop)	List contents of alarm counters on one or all DTI/PRI loops
LOVF c r	List threshold overflows for customer c (0-99) and route r (0-511)
RCNT	Reset alarm counters of all DTI/PRI loops
RCNT loop	Reset alarm counter of DTI/PRI loop
RMST loop	Perform self-test on loop
RMST l ch	Perform self-test on specified channel (2.0 Mb/s DTI/PRI only)
RLBK loop	Close loop at carrier interface point for testing
RLBK l ch	Close channel ch at carrier interface point
RSET l ch	Reset thresholds for channel ch
SLFT loop	Invoke hardware self-test on loop
SLFT l ch	Invoke partial hardware self-test on channel ch
STAT	Get status of all loops
STAT loop	Get status of DTI/PRI loop
STAT l ch	Get status of channel ch
VER (loop)	Query existing UDT card firmware version

Clock controller commands

DIS CC n	Disable system clock controller n
DSCK loop	Disables the clock for loop
DSYL loop	Disable yellow alarm processing for loop
ENCK loop	Enable the clock for loop
ENL CC x / l s	Enable system clock controller x OR superloop and shelf

<fdl>	
ENYL loop	Enable yellow alarm processing for loop
EREF	Enable automatic switchover of system clocks
IDC x	Get card ID of Clock Controller card in side x
MREF	Disable switchover of system clocks
RST CC x	Reset side x of the Downloadable Clock Controller
SEFT CC x	Execute a self test on side x of the Downloadable Clock Controller.
SLFT CC x	Execute a selftest on side x of the Downloadable Clock Controller
SSCK n / l s	Get status of system clock n OR superloop and card
<full>	
SWCK	Switch system clock from active to standby
SWCK FRCE	Force system clock to switch from active to standby
TRCK aaa n / l s	Set clock controller tracking to primary, secondary or free run

Alphabetical list of commands

Command	Description	Pack/Rel
ATLP (0), 1	Disable (0) or enable (1) daily routine auto loop test. Where: • 1 = loop test enable; causes far-end to raise and clear yellow alarm • 0 =run the partial loop test; there is no interaction for far-end loop (default value) LD 60 is included in the daily (midnight) routines if defined by LD 17 prompt DROL. ATLP is only run if LD 60 is included in the daily routines. If ATLP = 1, and all 24 channels on the loop are idle, then the DTI/PRI card is disabled and a self-test is performed on each channel. All DTI/PRI cards are tested, one at a time. If a D-channel is on the loop, it is temporarily released and reestablished. If one or more channels are busy, the test is not performed on the loop.	dti/pra-5

Command	Description	Pack/Rel
	If ATLP = 0, then an "AUTO TEST DSBL" message is output and only one channel is tested. The channel is randomly selected by software, it cannot be specified.	
CDSP	Clear maintenance display to 00 or blank.	dti/pra-5
CMIN	Clears minor alarm for all customers.	alrm_filter-22
CMIN ALL	Clears minor alarm for all customers.	dti/pra-5
DIS CC 0	Disable system clock controller. (does not apply to CS 1000E)	
DIS CC x (0,1)		dti/pra-5
	Disable system clock controller 0 or 1. (does not apply to CS 1000E) CPU 0 must be idle to disable CC 0. CPU 1 must be idle to disable CC 1. To switch CPUs, use the SPCU command in LD 135.	
DIS CC LP SHELF	Disable system clock. (CS 1000E only)	
DISI loop	Disable DTI/PRI loop when all channels are idle. The network and DTI/PRI cards are then disabled and status LEDs are lit. Channel status is set to BSY. Enter END to abort. When the PRI is physically connected to a DCHI card, the D-channels must be disabled first using LD 96.	dti/pra-5
DISL loop	Disable network and DTI/PRI/DTI2/PRI2 cards of loop. (PRI & PRI2 loops cannot be disabled unless associated D-channel is disabled first using LD 96). Active calls are force disconnected by on-hook simulation. All channels are disabled and status LEDs are lit.	dti/pra-5
DLBK loop	Disable remote loop back test per RLBK command. Loop remains disabled.	dti/pra-5
DLBK l ch	Disable remote loop back test per RLBK loop ch command. The channel remains disabled.	dti/pra-5
DSCH l ch	Disable channel ch of loop l.	dti/pra-5

Command	Description	Pack/Rel
DSCK loop	Disables the clock for loop, which does not have to be previously defined as the primary or secondary clock source.	dti/pra-5
DSYL loop	Disable yellow alarm processing for loop.	dti/pra-5
ENCH loop	Enable all channels on DTI2 loop.	dti/pra-5
ENCH l ch	Enable channel ch of loop. For TIE trunks with A+B signaling, the channel is set to the same state as the far-end. The far-end refers to the status of the channels as presented by DTI T1 port. With B-channel signaling, channels are placed into the IDLE state and made available for calls.	dti 2 - 5
ENCK loop	Enables the clock for loop, which must be previously defined as a primary or secondary clock source via service change.	dti/pra-5
END	Aborts the program.	dti/pra-5
ENL CC x / l s <fdl>	Enable system clock controller, where: x = 0 or 1 l s = superloop and card fdl = Force DownLoad for the NTRB53 card with Release 25.40 and later	dti/pra-5 basic-5.00
ENL CC LP SHELF	Enable system clock. (CS 1000E only)	
ENLL loop	Enable network and DTI/PRI/DTI2/PRI2 cards of loop. For TIE trunks with A+B signaling, the channels are set to the same status as the far-end; otherwise, the channels are set to idle status. The far-end refers to the status of the channels as presented by DTI T1 port. Status LEDs are deactivated. With B-channel signaling, channels are placed into the IDLE state and made available for calls.	dti/pra-5
ENYL loop	Enable yellow alarm processing for loop.	dti/pra-5
EREF	Enables automatic switchover of primary and secondary reference clocks. Also enables recovery to	dti/pra-5

Command	Description	Pack/Rel
	primary or secondary clocks when loops associated with these clocks are automatically enabled.	
IDC x	Get card ID of Clock Controller card in side x.	basic-25.4
LCNT (loop)	List contents of alarm counters on one or all of the following cases, where:	dti/pra-5
	loop = 0-255, System with Fibre Network Fabric	fnf-25
	Case 1 1.5 Mb/s DTI/PRI The counters are: • BPV = bipolar violation counter • SLIPD = frame slip deletion counter • SLIPR = frame slip repetition count • LOSFA = loss of frame alignment counter • OS_BPV = 24-hr bipolar violation counter - For PRI with D2, D3, or D4 framing format, 24-hr bipolar violation counter - For PRI with Extended Superframe Format, 24-hr Cyclic Redundancy Check (CRC) counter • OS_LOSFA = 24-hr loss of frame alignment counter • OS_YEL = 24-hr yellow alarm counter Case 2 2.0 Mb/S DTI The counters are: • G1 alarms • BPV = bipolar violation counter • FAP = frame alignment threshold counter • SLP = maintenance threshold slip counter • CRC = cyclic redundancy threshold counter • AIS = alarm indication signal • AIS64 = 64 Kb/s alarm indication signal • FAL = loss of frame alignment • MFAL = loss of multiframe alignment • BIT3 = bit 3 error • BIT6 = bit 6 error • CFAS = loss of crc-4 multiframe alignment	

Command	Description	Pack/Rel
	Case 3 2.0 Mb/s PRI The counters are: • BPV = bipolar violation counter • CRC = cyclic redundancy threshold counter • FAP = frame alignment threshold counter • SLP = maintenance threshold slip counter • AIS = alarm indication signal • LFAS = loss of frame alignment signal • LMAS = loss of multiframe alignment signal • RAI = remote alarm indication • LOS = loss of signal	
LOVF c r	List threshold overflows for customer c (0-99) and route r (0-511). The overflows are set when the resident trunk monitor outputs a diagnostic message. Defined thresholds are HOLD, ILLR, REPT, SEIZ and SVFL (see LD 16).	dti/pra-5
MREF	Disable switchover of system clocks. Also disables recovery to primary or secondary reference clocks when loops associated with these clocks are automatically enabled.	dti/pra-5
RCNT (loop)	Reset alarm counters for all or specified loop only. If the DTI loop was disabled due to an error threshold overflow and the DTI may be enabled automatically when the counter is cleared, then before performing any command, such as test, that requires the DTI to be disabled you should: 1. disable the DTI 2. list the counters with the LCNT command 3. reset the counters with the RCNT command 4. do the test commands	dti/pra-5
REST l	Perform self-test on specified loop l where: l = 0-255, System with Fibre Network Fabric	fnf-25
RLBK loop	Close loop at carrier interface point for testing. Allows the far-end to perform an external loop back test on the carrier span using the RMST command. This command closes the loop at the carrier interface	dti/pra-5

Command	Description	Pack/Rel
	point of the DTI/PRI. The DTI/PRI loop must be disabled first using the DISI or DISL loop commands.	
RLBK l ch	Close channel ch at carrier interface point. Allows the far-end to perform an external loop back test on the carrier span. The loop remains enabled, but closes the specified channel at the carrier interface point of the DTI/PRI. The DTI/PRI channel must be disabled first using the DSCH loop ch command.	dti/pra-5
RMST loop	Perform remote loop back test on loop. The far-end must be in the remote loop back mode. (RLBK command has been issued at the far-end)	dti/pra-5
RMST l ch	The far-end channel must be in the remote loop back mode. (RLBK command has been issued at the far-end)	dti 2 - 14
RSET l ch	Reset thresholds for channel ch on loop l.	dti/pra-5
SEFT CC x	Execute a self test on side x of the Downloadable Clock Controller.	basic-25.4
SLFT loop	Invoke DTI/PRI hardware self-test on loop. This command tests speech path continuity, zero code suppression, remote alarm detection, and A&B bit signaling. The loop must be disabled first using the DISI or DISL loop command.	dti/pra-5
SLFT l ch	Invoke partial hardware self-test on channel ch. The DTI/PRI channel must be disabled first using the DSCH command.	basic-1
SSCK x / l s <full>	Get status of system clock where: x = 0 or 1 l s = superloop and card full = Get full status of clock in side x, including serial number and loadware versions and states. The SSCK command indicates the active controller as well as active primary or secondary reference clock source or free run. Response may be:	dti/pra-5 basic-5.00 basic-25.4

Command	Description	Pack/Rel
	1. AUTO SWREF CLK – ENBL = automatic switchover of system clocks enabled 2. AUTO SWREF CLK – DSBL = automatic switchover of system clocks disabled 3. CLOCK ACTIVE = the active controller 4. DSBL = clock disabled 5. ENBL = clock enabled 6. REF CLK ERR = possible faulty cable from CC to DTI/PRI, or faulty Clock Controller 7. SYSTEM CLOCK - FREE RUN, PREF or SREF = clock is in free run mode or tracking to the primary (PREF) or secondary (SREF) reference loop 8. VCXO AGING ERROR = the timing crystal is faulty, replace the clock	
STAT	Get status of all digital loops. The types of loops are: 1. PRI = Primary Rate Interface 2. PRI2 =2.0 Mb/s Primary Rate Interface 3. DTI = Digital Trunk Interface 4. DTI2 =2.0 Mb/s Digital Trunk Interface 5. DLI = Digital Link Interface 6. JDMI = Japan Digital Multiplex Interface	dti/pra-5

STAT loop	Get status of digital loop. Sample output:
	`AAA TRK LOOP x – BBBB`
	`SERVICE RESTORE: YES/NO`
	`YEL ALM PROCESS: YES/NO`
	`ALARM STATUS: NO ALARM/RED(local) ALARM`
	Where: AAA may be :
	`1. DTI`
	`2. DTI2`
	`3. PRI`
	`4. PRI2`
	`5. TIE`
	`6. DID`
	`7. DTI LINK (DTI link loop = DLI)`
	Where: BBBB may be:
		dti/pra-5

Command	Description	Pack/Rel

1. DSBL = Hardware of specified digital loop is disabled
2. ENBL = Hardware of specified digital loop is enabled
3. RLBK = Hardware of specified digital loop is in remote loop back mode
4. DISI PENDING = DSI command is in progress
5. TRACKING = system clock is tracked to this loop
6. IDLE = Hardware of specified digital loop is idle
   When AAA = TIE, IDLE ISPC indicates that the channel is an established ISPC link ready to be used by any end-users having access to the associated ISPC route.
7. SERVER RCVY = server has not recovered status of DTI LINK loop. Channels will not be allocated for call processing until this status is removed by the server
8. BUSY = Hardware of specified digital loop is busy
   When AAA = TIE, BUSY ISPC indicates that the channel is an established ISPC link which is used by end users on the PBXs.
   When AAA = DID, BUSY ISPC indicates that the ISPC link is established to the Central Office. The status "BUSY" is independent to ISL feature usage of the ISPC link.
9. MSBY = Hardware of specified digital loop is in make busy mode
   When AAA = TIE, MSBY ISPC indicates that the configured ISPC link is one of the following:
   a. not established yet
   b. established, but the ISL D-channel which controls its usage not established

Where: SERVICE RESTORE may be:

1. YES = restore service automatically if alarm is removed
2. NO = loop can only be manually enabled

Where: YEL ALARM PROCESS may be:

1. YES = yellow alarm processing is enabled
2. NO = yellow alarm processing is disabled

Command	Description	Pack/Rel
	Where: ALARM STATUS may be: 1. NO ALARM = no alarm active 2. RED = red (local) alarm active Action 1: 1. list alarm counters (LCNT command) 2. check for DTA messages 3. go to the fault clearing section Where: • YELLOW = yellow (remote) alarm active • WAITING = DTI/PRI card is not responding. The card either did not respond to a status check or did not respond when a red alarm was cleared. Go to Action 2. Action 2: 1. check DTI/PRI status again 2. disable, then enable the DTI/PRIPRI STATE OF SERVICE: • OOS = out-of-service • NNC = no new call • NNDC = no new data call • MNT = maintenance When an alarm is present (group 2 error), it is a REMOTE ALARM REMOTE ALARM: • NS = alarm indication signal • RAI = remote alarm indication LOCAL ALARM: • LOS = loss of signal • LFAS = loss of frame alignment signal • LMAS = loss of multiframe alignment signal	
STAT l ch	Get status of channel ch. Status may be:	dti/pra-5

Command	Description	Pack/Rel
	1. IDLE = channel is enabled and is idle 2. BUSY = channel is enabled and is call processing busy or channel is in a lockout state (far-end is disabled) 3. MBSY = channel is being used for maintenance busy, the D-channel is down, or far-end channel is disabled 4. DSBL = channel is disabled 5. DSBL (SERVER) = channel is being used for server maintenance and is disabled for the duration (1.5 Mb/s DTI digital link interface only) 6. FE MBSY = near end is idle, far-end is maintenance busy 7. FE DSBL = near end is idle, far-end is disabled 8. FE DSBL = far-end B-channel is disabled 9. FE MBSY = far-end B-channel is in maintenance mode 10. UNEQ = channel is not equipped When the loop is a Phantom loop, it is possible to receive the status messages: TIE IDLE ISPC, TIE BUSY ISPC , or TIE MSBY ISPC . Interpret these system responses as they are interpreted for the command STAT loop. See the section which outlines BBBB alternatives for the STAT loop command on 1 on page 277.	
SWCK	Switch system clock from active to standby. The reference clock source remains unchanged. **Note:** Wait 2 to 3 minutes between clock switches. Ensure both clock controllers are locked by using SSCK (LD 60) before a manual clock switch is performed..	dti/pra-5
SWCK FRCE	Force system clock to switch from active to standby. Functions with NTRB53 Clock Controller **Note:** Switch occurs regardless of 1 minute clock switch timer being set, or a FIJI alarm preventing a switch is on.	basic-3.0

Command	Description	Pack/Rel
TRCK aaa n / l s	Set clock controller tracking. Where aaa is: • PCK = track primary clock (on remote) • SCLK = track secondary clock (on remote) • FRUN = free run mode • PLL1 = track on port 1 IP connection to/from Main • PLL2 = track on port 2 IP connection to/from Main • PLL3 = track on port 3 IP connection to/from Main • PLL4 = track on port 4 IP connection to/from Main Where n is: • 0 = Main cabinet clock • 1, 2, 3, or 4 = IP expansion cabinet or MG 1000S number Where l s is: l s = superloop and shelf Parameters PLL1, PLL3 and PLL4 can be used with n=0 only. Track primary clock (PCK) or secondary clock (SCLK) as the reference clock or go to free run (FRUN) mode.	dti/pra-5 basic-5.00
VER (loop)	Query existing UDT card firmware version. UDT loop should be in enabled state in order to successfully perform the command. The response format is: UDT <loop> VER <AAnn>	basic-6.00

Chapter 25: LD 61: Message Waiting Lamps Reset

The Message Waiting Lamps Reset (MWL) program can be invoked automatically by the system as part of the daily routines or manually from an input device. It is used to deactivate all active Message Waiting lamps on user stations and reset the associated status in the system.

This program cannot be applied to digital sets.

When LD 61 is loaded manually, 'G' must be entered to initiate the task.

G command

Starts resetting the trouble status on all Message Waiting lamps. The program does not reset lamp status unless all message center sets are out-of-service (i.e., message center is closed and attendants are in Night Service).

Before running this program, all Message Center (MC) telephones must be taken out-of-service by "make telephone busy" and if attendants are set up to handle message calls, they must be in night mode.

Chapter 26: LD 75: Digital Trunk Maintenance

This program lets you test digital channels, bring a digital (IDA) link into service or take a link out-of-service.

All Overlay 75 commands may be used on Small Systems, CS 1000S, systems by substituting card number for loop number.

Basic commands

CDSP	Clears the maintenance display
CMIN	Clears minor alarm for all customers.
CMIN ALL	Clears minor alarm for all customers.
DIS DDCS loop	Disables DDCS loop
DIS DDSL n	Disables DDSL n
DIS DTCS loop	Disables DTCS loop
DIS DTRC l c	Disables real channel c on loop l
DIS DTSL n	Disables DTSL n
DIS DTVC l c	Disables virtual channel c on loop l
DIS LSSL n	Disables Low Speed Signaling Link n for APNSS
DIS MON l	Disables monitoring of level 3 messages on a DDSL loop l
DIS MSGI	Disables monitoring of incoming messages for all DDSL
DIS MSGO	Disables monitoring of outgoing messages for all DDSL
DIS PRI2 loop	Disables PRI2 loop
DISI DDCS loop	Disables all channels on loop as they become idle
DISI DTCS loop	Disables all channels on loop as they become idle
ENL DDCS loop	Enables DDCS loop
ENL DDSL n	Enables DDSL n
ENL DTCS loop	Enables DTCS loop

ENL DTRC l c	Enables real channel c on loop l
ENL DTSL n	Enables DTSL n
ENL DTVC l c	Enables virtual channel c on loop l
ENL LSSL n	Enables Low Speed Signaling Link n for APNSS
ENL MON l	Enable monitoring of level 3 messages on a DDSL loop l in long format
ENL MON l aaaa	Enable monitoring of level 3 messages on a DDSL loop l in aaaa formats
ENL MSGI	Enable monitoring of incoming messages for all DDSL loops
ENL MSGO	Enable monitoring of outgoing messages for all DDSL loops
ENL PRI2 loop	Enables PRI2 loop
RCNT (ddsl)	Reset alarm counters for a specified DDSL only
STAT DDCS (loop)	Gives status of all DDCS loops if loop omitted. Gives status of DDCS loop and all channels on loop if loop specified.
STAT DDSL (n)	Gives status of all DDSLs if n omitted. Gives status of DDSL n if n specified.
STAT DTCS (loop)	Gives status of all DTCS loops if loop omitted. Gives status of DTCS loop and all channels on loop if loop specified.
STAT DTRC l c	Gives status of real digital channel c on loop l
STAT DTSL (n)	Gives status of all DTSLs if n omitted. Gives status of DTSL n if n specified.
STAT DTVC l c	Gives status of virtual digital channel c on loop l
STAT LSRC n (x)	Gives status of Real Channel x on Signaling Link n
STAT LSSL n	Gives status of Low Speed Signaling Link n for APNSS
STAT LSVC n (x)	Gives status of Virtual Channel x on Signaling Link n
STAT PRI2 loop	Status of PRI2 loop
STRT n	Starts DDSL n

Note:
If GEC Plessey Telecommunications (GPT) hardware is used, the mnemonic DTSL is used instead of DDSL and the mnemonic DTCS is used instead of DDCS.

Alphabetical list of commands

Command	Description	Pack/Rel
CDSP	Clears the maintenance display.	dpnss-16
CMIN	Clears minor alarm for all customers.	alrm_filter-22
CMIN ALL	Clears minor alarm for all customers.	dpnss-16
DIS DDCS loop	Disables DDCS loop.	dpnss-16
DIS DDSL n	Disables DDSL n.	dpnss-16
DIS DTCS loop	Disables DTCS loop	dpnss-16
DIS DTRC l c	Disables real channel c on loop l.	dpnss-16
DIS DTSL n	Disables DTSL n.	dpnss-16
DIS DTVC l c	Disables virtual channel c on loop l.	dpnss-16
DIS LSSL n	Disables LSSL n.	dpnss-16
DIS MON loop	Disables monitoring of level 3 messages on a DDSL loop	
DIS MSGI	Disables monitoring of incoming messages for all DDSL	dpnss-24
DIS MSGO	Disables monitoring of incoming messages for all DDSL	dpnss-24
DIS PRI2 loop	Disable PRI2 loop	basic-5.00
DISI DDCS loop	Disables all channels on loop as they become idle. The message "OK DISABLING" is issued and further commands can be entered. DTM055 is issued when all of the channels are disabled.	dpnss-16
DISI DTCS loop	Disables all channels on loop as they become idle.	dpnss-16
ENL DDCS loop	Enables DDCS loop.	dpnss-16

Command	Description	Pack/Rel
ENL DDSL n	Enables DDSL n.	dpnss-16
ENL DTCS loop	Enables DTCS loop.	dpnss-16
ENL DTRC l c	Enables real channel c on loop l.	dpnss-16
ENL DTSL n	Enables DTSL n.	dpnss-16
ENL DTVC l c	Enables virtual channel c on loop l.	dpnss-16
ENL LSSL n	Enables Low Speed Signaling Link n for APNSS.	dpnss-16
ENL MON l	Enables monitoring of level 3 messages on a DDSL loop l (by default, both incoming and outgoing messages are monitored)	dpnss-24
ENL MON l aaaa	Enable monitoring of level 3 messages on a DDLS loop l. Where aaaa can be one of the following: • shrt = short format • long = long format • decd = decoded format	dpnss-24
ENL MSGI	Enables monitoring of incoming messages for all DDSL loops	dpnss-24
ENL MSGO	Enables monitoring of outgoing messages for all DDSL loops	dpnss-24
ENL PRI2 loop	Enable PRI2 loop	basic-5.00
RCNT (ddsl)	Reset alarm counters for a specified DDSL only, where: ddsl = IDA, DASS, DASS2, DPNSS	dpnss-25
STAT DDCS (loop)	Gives status of all DDCS loops if loop omitted. Gives status of DDCS loop and all channels on loop if loop specified.	dpnss-16
STAT DDSL (n)	Gives status of all DDSLs if n omitted or specified.	dpnss-16
STAT DTCS (loop)	Gives status of all DTCS loops if loop omitted. Gives status of DTCS loop and all channels on loop if loop specified.	dpnss-16
STAT DTRC l c	Gives status of real digital channel c on loop l	dpnss-16

Command	Description	Pack/Rel
STAT DTSL (n)	Gives status of all DTSLs if n omitted. Gives status of DTSL n if n specified.	dpnss-16
STAT DTVC l c	Gives status of virtual digital channel c on loop l	dpnss-16
STAT LSRC n (x)	Gives status of Real Channel x on Signaling Link n	dpnss-16
STAT LSSL n	Gives status of Low Speed Signaling Link n for APNSS	dpnss-16
STAT LSVC n (x)	Gives status of Virtual Channel x on Signaling Link n	dpnss-16
STAT PRI2 loop	Status of PRI2 loop	basic-5.00
STRT n	Starts DDSL n The message "OK, STARTING" is issued and further commands can be entered. DTM301 is issued when the link is successfully started.	dpnss-16

Chapter 27: LD 77: Manual Print

LD 77 is used to print the signals that come from the peripheral cards to the common equipment.

Note:
This Overlay is intended for people experienced with the message formats and protocols.

Some loop-level commands are not valid on Small Systems, CS 1000S, MG 1000B, and MG 1000Tsystems, and have been replaced with slot-level commands.

When to use LD 77

LD 77 can be useful in determining which peripheral card (line or trunk) is causing a system overload in situations in which the CPU cannot narrow the problem to a specific Terminal Number (TN). Once the program is loaded from a tape, the user may request the system to print all the input messages from a specific area of Intelligent Peripheral Equipment.

Manual Print can also be used to continuously send frequency combinations by defining the loop and terminal number of the MFE card, busying the channel, setting the read/write bit to write, defining the message and repeatedly sending it. This channel will not be available for regular signaling until the message sending is stopped and the channel is idled.

When a machine is carrying traffic, there will be a large number of valid messages generated from the Intelligent Peripheral Equipment. Thus, the program will be most effective for trouble-shooting when:

- there is little system traffic
- message address range is restricted (i.e., looks only at one shelf or loop)

This program has capabilities which are used by the software designers during development activities. The user is protected from accidental access to these commands (and resulting potential service degradation) as a password is required. This password is not available to customers.

LD 77 Output format

All numerical input/output is in hexadecimal format. The output is in the following format:

<loop> <shelf> <card> <terminal> <message> <time-stamp>

The loop, shelf and card fields identify the circuit card generating the message.

Abbreviations for LD 77

The fields are defined as follows:

b = bypass bit value

cb = continuity bit

ch = chip on a given SSD Peripheral Signaling card

g = group

l s c u = TN: loop, shelf, card, unit

ln = link

loop = network loop

m = module

p = page

ps = Peripheral Signaling card

sh = Multigroup shelf

ts = time slot

v = desired lamp state; 0 = lit, 1 = dark

x = Multigroup bit

Some four-letter commands can be abbreviated to a one-letter command when entered from a TTY (but not an SL-1 telephone). The one-letter command is shown in parentheses after the four-letter mnemonic (e. g., ARPS (F) l s 32 can be entered as F l s 32).

LD 77 Input format

All input is in decimal form, except message data which is in hexadecimal form. Space and carriage return are automatically done by the overlay when the expected number of digits are input. Therefore the number of input digits must be strictly entered for each input parameter. The number of letters specified in each parameter field dictate the number of hex or decimal digits that must be entered.

For example:

Enter for TN 1 0 2 0:

001 0 02 00

Enter for TN 156 1 15 30:

156 1 15 30

Fibre Network Fabric

The Fibre Network Fabric extends and enhances the 5-group network architecture to 8 non-blocking (inter-group) Network groups, with a resulting expansion in network capacity to 8k timeslots available for Intergroup traffic. This is achieved by using OC-12 SONET rings, and adding additional network and IPE shelves, cards and cables and software changes to allow using the expanded network capacity. This expansion increases the number of available loops from 160 to 256. This applies to Multi Group systems only.

Basic commands

Only "P" commands can be used on superloops.

ANWK (B) loop ts	Read/write network card memory
ANWS (C) loop ts	Read/write network card memory (short)
ARPM loop 20	Print contents of timeslots in RPC
ARPM loop ts b s c u	Get contents of timeslot ts, loop
ARPS (F) loop ts	Read Remote Peripheral Switch memory
DFTM (T) s c u	Define unit to receive signaling messages
DLMP 0/1	Turn on/off lamp audit
DMTN	Monitor input and output SSD messages for 1 to 6 TNs
DISC	Call disconnect
DRTM (N) l s c u	Stop printing messages
KALL	Call set up without specifying timeslots
KALS	Call set up with specifying timeslots
KILLx	Reset one or all TN being monitored
N	Stop print

P	Print all messages
P lll	Print all messages from specified loop lll
P lll s	Print all messages from specified shelf lll s
P lll s cc	Print all messages from specified card lll s cc
PRTM (P) l s c u	Print messages, as specified l s c u
IMSG	Send input SSD messages from IPE to system CPU
WCTS loop	Print the current unit scan of loop
WMBY l s c u	Write the maintenance bit for the given unit to BUSY
WMUB l s c u	Write the maintenance bit for the given unit to NOT BUSY
XMSG	Send output SSD messages from system CPU to IPE
XMII, XMIO	Send input/output XMI messages between the CPU and superloops
XRCL loop	Read contents of RPC control register for loop
XRSH loop	Read and print contents of SHEN register for loop
XRST loop	Read and print contents of STATUS register for loop
XTRP loop	Test remote RPC processor for loop
XTLP loop	Test local RPC processor for loop
XWCS loop xxxx	Writes RPC control/SHEN register for loop

Alphabetical list of commands

Command	Description	Pack/Rel
ANWK (B) loop ts		basic-1
	Read/write network card memory. Access the specified network card memory to read and print one word. The word format is <cb s c u x ln -->, where: • cb = continuity bit • s = shelf • c = card • u = unit • x = multigroup bit • ln = link	

Command	Description	Pack/Rel
	You can write in new data. To change the values, rekey the word after the dashes, substituting new values where appropriate.	
ANWS (C) loop ts		basic-1
	Read/write network card memory (short). Access the specified network card memory (short form) to read and print one word. The multigroup bit and continuity field are not used. The word format is: <s c u ln -->, where: • s = shelf • c = card • u = unit • ln = link. You can write in new data. To change the values, rekey the word after the dashes, substituting new values where appropriate.	
ARPM loop 20		
	Prints contents of 32 timeslots in RPC associated with loop (20 hexadecimal = 32 decimal).	basic-1
ARPM loop ts b s c u		basic-1
	Get contents of timeslot ts, loop. The system prints data in the form "bscu", where b is the current value of the bypass bit in the Remote Peripheral Equipment Controller (RPC) memory (0 or 1) for that shelf, card and unit. The user can enter a new bypass bit for the RPC memory after the dash.	
ARPS (F) loop ts		basic-1
	Read Remote Peripheral Switch memory. Access the specified Remote Peripheral Switch (RPS) memory to read and print one word. The word format is: <cb s c u -->, where: • cb = continuity bit • s = shelf • c = card • u = unit. You can write in new data. To change the values, rekey the word after the dashes, substituting new values where appropriate.	
DFTM (T) s c u		basic-1
	Define unit to receive signaling messages.	

Command	Description	Pack/Rel

DISC	Call disconnect. Format is:
	`DISC`
	`TN1 l s c u`
	`TN2 l s c u`
	This command disconnects the call specified by the TNs. Ascan of the connection memory is done prior to disconnecting the call, if no timeslot can be found for the specified TN, nothing is done. TN1 and TN2 are prompted by the program.
		xpe-15

DLMP 0/1	Turn on/off lamp audit. Format is: • `DLMP 0` = turn on lamp audit • `DLMP 1` = turn off lamp audit	xpe-15
DMTN	Monitor input and output SSD messages for 1 to 6 TNs. This command is used to monitor all SSD messages for the specified TN. TN is automatically prompted by the program. Up to 6 TNs can be monitored at the same time. Enter the DLPM and DMTN commands as follows: DLMP 2 DMTN TNx l s c u TNx Loop 0 00 CH (Digital Trunk Cards), where: x = (1-6), TN index The output format is: `OSSD111 TN MSG TIME` , where: • `OSSD111` = header • `TN` = packed TN • `MSG` = SSD message content • `TIME` = real time clock before output when work scheduler gets the input message	xpe-15
DPRT c ch	Print messages from this digital channel (Small System, CS 1000S, MG 1000B,MG 1000T).	xpe-15
DPRT card	Print messages from this digital card. (Small System, CS 1000S, MG 1000B,MG 1000T).	xpe-15
DRTD c ch	Stop printing messages from this digital channel. (Small System, CS 1000S, MG 1000B,MG 1000T).	xpe-15
DRTD card	Stop printing messages from this digital card (Small System, CS 1000S, MG 1000B,MG 1000T).	xpe-15
DRTM (N) l s c u		basic-1

Command	Description	Pack/Rel
	Stop printing messages from the loop, shelf, card and unit. Only loop and shelf numbers are required.	
IMSG	Send input SSD messages from IPE to system CPU. This command is used to simulate incoming SSD message from the Intelligent Peripheral Equipment. The specified TN must be equipped. Format is: `IMSG TN l s c u NUMBER MESSAGES mm # TIMES TO SEND hhh MSG DATA xxxx xxxx xxxx xxxx. . .` where: • `mm` = number of SSD messages (1-10) to be sent • `hhh` = number of times (1-999) to simulate the SSD input message • `xxxx` = SSD message content. Number of message contents depends on input of mm `TN, NUMBER MESSAGES, # TIMES TO SEND` , and `MSG DATA` are prompted by the program.	xpe-15
KALL	Call set up without specifying timeslots. This command is used to set up a simple call (intra or inter-group). The system finds an available timeslot for the specified TNs. The specified TN must be equipped, enabled and idle. Format is: `KALL TN1 l s c u, TN l s c u Loop 0 00 CH` for Digital Trunk Cards. `TN2 l s c u, TN l s c u Loop 0 00 CH` for Digital Trunk Cards. `TN1` and `TN2` are automatically prompted by the program. If AUDIT is running, call(s) are disconnected, and AUD17, AUD18, AUD19, and/or AUD31, AUD32 is printed. Call setup command simply finds the available timeslots and sets up the connection memory and/or junctor memory. BUG105, BUG330 may be printed if illegal sequences are carried out. These commands are designed for lab use only, and should be used cautiously in a live switch.	xpe-15
KALS	Call set up with specifying timeslots. This command will set up a call specified by the input TNs and the timeslots if both TNs are equipped, enable and idle. The specified timeslots will be used if they are idle, if the specified timeslot are occupied, then the call will not be set up. See Notes with the KALL command. Format: `KALS`	xpe-15

Command	Description	Pack/Rel
	TN1 l s c u, TN l s c u, Loop 0 00 CH for Digital Trunk Cards. TN2 l s c u, TN l s c u, Loop 0 00 CH for Digital Trunk Cards. TIMESLOTS ts1 ts2 Where: • ts1 = specified timeslot of the TN1 • ts2 = specified timeslot of the TN2 • TN1, TN2 , and TIMESLOTS are prompted by the program.	
KILLx	Reset one or all TN being monitored. Where: x = the TN index number (1-6) entered with the DMTN command. Enter 7 to reset all the output monitored TNs.	xpe-15
N	Stop print.	basic-1
P	Print all messages.	basic-1
P lll	Print all messages from specified loop. Enter the exact number of digits. Example: for loop 4, enter 004	basic-1
P lll s	Print all messages from specified shelf. Enter the exact number of digits. Example: for loop 4, enter 004.	basic-1
P lll s cc	Print all messages from specified card. Enter the exact number of digits. Example: for loop 4, enter 004.	basic-1
PRTM (P) l s c u	Print messages, as specified. Only loop and shelf numbers are required. Enter the exact number of digits. (Example: for loop 4, enter 004.)	basic-1
WCTS loop	Print the current unit scan of specified loop. Outputs shelf, card and unit.	basic-1
WMBY l s c u	Write the maintenance bit for the given unit to BUSY.	basic-1
WMUB l s c u	Write the maintenance bit for the given unit to NOT BUSY.	basic-1

Command	Description	Pack/Rel

XMII, XMIO	Send input/output XMI messages between the CPU and superloops.
	Send input/output XMI messages to the Peripheral Controller (NT8D01) or Network card (NT8D04). Use XMII for input messages from the Network card (NT8D04) to the CPU. Use XMIO for messages from the CPU to the Network.
	This command is used to simulate input/output XMI message. It may not be useful in LD 77.
	Format:
	`XMII or XMIO`
	`LOOP lll`
	`NUMBER MESSAGES m`
	`# TIMES TO SEND hhh`
	`MSG DATA`
	`cccc xxxx xxxxxxxx`
	`cccc xxxx xxxxxxxx`
	`cccc xxxx xxxxxxxx`
	Where:
	• `lll` = Loop number
	• `m` = Number of multiple XMI messages (1-6)
	• `hhh` = Number of times to send XMI messages (1-999)
	• `cccc` = Control word; cccc is defined as follows:
	`r ss applic type`
	`- | -- | ------ | ------- |`
	Where:
	• `r` = one bit msg ready flag, always sets to
	• `ss` = two bit sequence status field. ss may be:
	a. B.00 : short message
	b. B.01 : starting a long message (message has 6 or more words of data)
	c. B.10 : continue a long msg
	d. B.11 : end of a long msg
	• `applic` = six bit value for msg's intended application. appl may be:
	a. B.000001 : for LD 30
	b. B.000010 : for LD 32
	c. B.000011 : for LD 45
	d. B.000100 : for LD 77
	e. B.000101 : for XPE parameter download
		xpe-15

Command	Description	Pack/Rel
	f. B.000110 : for XNET action request • `type` = seven bit value of message type • `xxxx` = message data	

XMSG	Send output SSD messages from system CPU to IPE. This command is used to send output SSD message to the Intelligent Peripheral Equipment TN. The specified loop of the TN must be enabled and responding.
	Format:
	`XMSG`
	`TN l s c u,`
	`TN l s c u,`
	`Loop 0 00 CH for Digital Trunk Cards.`
	`NUMBER MESSAGES mm`
	`# TIMES TO SEND hhh`
	`MSG DATA xxxx xxxx xxxx. . . .`
	Where:
	• `mm` = number of SSD messages to be sent (1-10)
	• `hhh` = number of times to output SSD message (1-999)
	• `xxxx` = SSD message content. Number of message contents depends on the value of mm
	• `TN, NUMBER MESSAGES, # TIMES TO SEND` , and `MSG DATA` are prompted by the program.
		xpe-15

XRCL loop	Read contents of RPC control register.	basic-1
XRSH loop	Read and print contents of SHEN register.	basic-1
XRST loop	Read and print contents of STATUS register.	basic-1
XTLP loop	Test local RPC processor for loop.	basic-1
XTRP loop	Test remote RPC processor for loop.	basic-1
XWCS loop xxxx	Writes RPC control/SHEN register for loop with data xxxx in hexadecimal format.	basic-1

Chapter 28: LD 80: Call Trace

LD 80 provides a means of tracing a call by looking at a snap shot of the transient data (such as call register contents) associated with the call. The trace commands operate only when this Overlay is active. If LD 80 is aborted (****), the trace functions stop. Note that when using the enhanced trace commands, the Overlay will not automatically abort (according to the defined time-out period) if calls are being traced.

When a system initialization occurs, all trace commands are removed, and the trace operation is stopped.

For Network Call Trace see NCT messages.

Enhanced Trace commands.

The enhanced trace function requires Multi-User Login functionality (package 242) to be enabled in LD 17. The enhanced commands are: DALL, DIST, ENTC, ENTD, GOTR, FITR, and STPT. These commands interact with each other only.

The enhanced trace commands can be disabled through a maintenance telephone by dialing the following: nn + 9913 + x + yy

Where:

- nn = customer SPRE access code
- 9913 = feature code to display for message display control
- x = action code (0 to deactivate)
- yy = message monitor code (02 for enhanced trace messages)

A second dial tone indicate that the command was successful. Overflow tone is heard if the command is entered incorrectly. Once this command has been entered, a user entering FITR from the TTY will receive the period (.) prompt.

Some loop-level commands are not valid on Small Systems, CS 1000S, MG 1000B, and MG 1000T, and have been replaced with slot-level commands.

Calling Line ID on Analog Trunks for Singapone, Australia and Hong Kong

The TRAC program will display the Calling Number for an incoming A-CLID call. Calling Name cannot be displayed.

If the calling number is not received i.e. "P" or "O" received as reason for absence of calling number then the route and member number will be displayed as per the existing functionality.

When to use LD 80

There are three basic commands:

- TRAT for tracing attendant consoles
- TRAC for tracing sets and trunks
- TRAD for tracing calls through Computer PBX Interface (CPI), Digital Trunk Interface (DTI), Primary Rate Interface, or Digital Link Interface (DLI) loops.

The TRAC command can be used to print the tone detector TN if a tone detector is used at the time of the call trace.

Generic software enables the printing of auxiliary data related to a call. The auxiliary data consists of information associated with the NARS/BARS/CDP features, if equipped, and the Ring Again (RGA) feature. This additional data can be retrieved by appending DEV to any of the TRAC commands. Example: TRAC L S C U DEV

Note:
BRI DNs can be traced with the TRAC C DN command. For TRAC L S C U, enter U = DSL0 to DSL7 for Digital Subscriber Loops.

When Music and Recorded Announcement Broadcast trunks are traced, the following information is printed out:

- indication that the trunk is broadcasting
- the number of callers connected to the trunk

When a caller connected to a broadcasting trunk is traced, the existing trace information is printed out as well as an indication that the trunk is broadcasting.

Originating and terminating information

The Call Trace originating and terminating party information depends on the types of telephone, console or trunk as shown below.

Single line telephones:

ORIG l s c u cust dn 500 TERM l s c u cust dn 500

Multi-line telephones:

ORIG l s c u key# keytype cust dn settype TERM l s c u key# keytype cust dn settype

Attendant consoles

ORIG l s c u cust att# lpk# ATTN consoletype TERM l s c u cust att# lpk# ATTN consoletype

Trunks:

ORIG l s c u rtyp RMBR rrr mmm TERM l s c u rtyp RMBR rrr mmm

- l s c u = TN
- consoletype = console type (ATT, 2250)
- cust = customer number
- dn = directory number
- key# = multi-line telephone key number
- keytype = multi-line telephone key type (SCR, MCR, HOT, etc.)
- lpk# = console loop key number
- rrr mm = trunk route and member number
- rtyp = trunk route type (TIE, CO, FX, etc.)
- settype = multi-line telephone type (SL1, 2008, 2317, etc.)

Example 1 Trace a call placed to a 500-type set

Configuration: active call from key 0 on an M2008, to 500-type telephone Customer number: 06

Originator:

telephone type: M2008 TN: 004 0 05 00 DN: 5100 on SCR key 0

Terminator:

telephone type: 500 TN: 008 0 03 06 DN: 2121

Trace command:

TRAC 4 0 5 0 (l s c u), or TRAC 6 5100 (customer and DN)

Output:

```
ACTIVE TN 004 0 05 00
ORIG 04 0 0 05 00 6 SCR 0 5100    2008
TERM  008  0  03   06     6   2121   500
DIAL DN 2121
MAIN PM   ESTD
TALKSLOT  ORIG 22    TERM 22
QUEUE NONE
```

Example 2 Trace an outgoing ISDN call

Configuration: outgoing call from key 0 on an M2317, to 500-type telephone Customer number: 05

Originator:

telephone type: M2317 TN: 016 0 02 00 DN: 6050 on SCR key 0

Terminator:

Dialed DN: 7873107 Outgoing PRI TIE trunk: loop 018 channel 16; route 24 member 12

Trace command:

TRAC 5 6050 (customer, DN), or TRAC 16 0 2 0 (l s c u)

Output:

```
ACTIVE  TN   016  0  02  00
ORIG     016  0  02  00      5   SCR 0    6050    2317
TERM     018  16     TIE  RMBR  24  12
DIAL DN  7873107
MAIN PM   ESTD
TALKSLOT  ORIG 13    TERM 13
QUEUE  NONE
---- ISDN PRA CALL (TERM) ----
CAL REF # = 16
BEARER CAP = VOICE
CALL STATE = 10     ACTIVE
CALLING NO = 4376050
CALLED NO = 7873107
```

Example 3 Enhanced Trace command output

The enhanced call trace output includes a time stamp that appears on the first line of the output.

The TN or digital trunk prints out only when there has been a change to the call register. The TN or trunk is printed only once.

Sample output:

```
.14:00:02 12/25/1992
KEY 0 MCR MARP ACTIVE TN 001 0 02 01
ORIG 001 02 01 0 SCR MARP 1 5011 SL1
TERM 001 0 02 00 0 MCR MARP 1 5006 SL1
DIAL DN 5006
MAIN_PM ESTD
TALKSLOT ORIG 19 TERM 21
QUEU NONE
KEY 1 TRN IDLE
KEY 2 AO3 IDLE
.
.
.
KEY 8 RND
KEY 9 RLS
.14:00:04 12/25/1992
IDLE TN 015 04
```

Example 4 Trace a call from an IP Media Services Ad Hoc Conference loop:

The call trace output includes the Media Application Server (MAS) IP address.

Trace command:

.trac 0 3000

Sample output:

```
ACTIVE VTN 104 0 00 00 ORIG CONF SERVICE 3 CONFEREE GRP 15 CALL ID 0
34999 ORIG 3 15 CONFEREE PORT 10 MAS IP: 47.11.58.228 PORT: 53652
MEDIA PROFILE: CODEC G.711 MU-LAW PAYLOAD 20 ms VAD OFF TERM VTN 104
0 00 00 KEY 0 SCR MARP CUST 0 DN 3000 TYPE 2002P2 SIGNALLING
ENCRYPTION: INSEC MEDIA ENDPOINT IP: 47.11.72.125 PORT: 5200 MEDIA
PROFILE: CODEC G.711 MU-LAW PAYLOAD 20 ms VAD OFF MAIN_PM ESTD
TALKSLOT ORIG 10 TERM 10 JUNCTOR ORIG0 TERM0 ORIG 3 15 CONFEREE PORT
8 MAS IP: 47.11.58.228 PORT: 53664 MEDIA PROFILE: CODEC G.711 MU-LAW
PAYLOAD 20 ms VAD OFF
```

VoIP Trace command output

Static Call Trace Output for calls involving IP Telephony elements.

Example 1 Trace a call placed from IP Phone to IP Phone within a single system

Trace command:

```
.trac 2 2222
```

Output:

```
ACTIVE  VTN 061 0 00 08
ORIG   VTN 061 0 00 04  KEY 0  SCR MARP  CUST 2  DN 2001  TYPE I2002
  MEDIA ENDPOINT IP: 192.168.64.33  PORT: 5200
TERM   VTN 061 0 00 08  KEY 0  SCR MARP  CUST 2  DN 2222  TYPE I2004
  MEDIA ENDPOINT IP: 192.168.64.32  PORT: 5200
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 20 ms  VAD OFF
DIAL DN 2222
MAIN_PM  ESTD
TALKSLOT  ORIG  8   TERM  10
EES_DATA:
NONE
QUEU  NONE
CALL ID 0 679
```

Example 2 Trace a Outgoing Virtual Trunk Call between TDM Phone and VGW Resource on Different Systems

Trace command:

```
.trac 1 1010
```

Output:

```
ACTIVE  TN 004 0 00 10
ORIG   TN 004 0 00 10  KEY 0 SCR MARP  CUST 1 DN 1010  TYPE 2616
  VGW TN 001 0 00 00
  MEDIA ENDPOINT IP: 192.168.64.22  PORT: 5200
TERM   VTN 062 0 00 09   VTRK IPTI  RMBR  70 10 OUTGOING VOIP GW CALL
  FAR-END H.323 SIGNALLING IP: 192.168.64.24
  FAR-END MEDIA ENDPOINT IP: 192.168.64.33  PORT: 5200
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 20 ms  VAD OFF
DIAL DN 2001
MAIN_PM  ESTD
TALKSLOT  ORIG  16   TERM  16
EES_DATA:
NONE
QUEU  NONE
CALL ID 0 707
```

Example 3 Trace an Incoming Virtual Trunk Call between two different systems

Trace command:

```
.trac 2 2001
```

Output:

```
ACTIVE  VTN 061 0 00 04
ORIG   VTN 082 0 00 00   VTRK IPTI  RMBR  100 1 INCOMING VOIP GW CALL
  FAR-END H.323 SIGNALLING IP: 192.168.64.20
  FAR-END MEDIA ENDPOINT IP: 192.168.64.22  PORT: 5200
TERM   VTN 061 0 00 04  KEY 0 SCR MARP  CUST 2 DN 2001  TYPE I2002
  MEDIA ENDPOINT IP: 192.168.64.33  PORT: 5200
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 20 ms  VAD OFF
DIAL DN 2001
MAIN_PM  ESTD
TALKSLOT  ORIG  83   TERM  16
EES_DATA:
NONE
QUEU  NONE
CALL ID 0 706
NETWORK  CALL ID  0 707
```

Example 4 Trace an IP Phone to Local TDM Device

Trace command:

```
.trac 2 2001
```

Output:

```
ACTIVE  VTN 061 0 00 04
ORIG   VTN 061 0 00 04  0  SCR MARP  2  2001  I2002
  MEDIA ENDPOINT IP: 192.168.64.33  PORT: 5200
TERM   TN 004 0 00 12  0  SCR MARP  2  2010  2616
  VGW TN 001 0 00 18
  MEDIA ENDPOINT IP: 192.168.64.22  PORT: 5236
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 20 ms  VAD OFF
DIAL DN 2010
MAIN_PM  ESTD
TALKSLOT  ORIG  49   TERM  17
EES_DATA:
NONE
QUEU  NONE
CALL ID 0 678
```

Example 5 Trace a call scenario between two Avaya Communication Server 1000E Media Gateways:

Trace command:

```
.trac 1 1006
```

Output:

```
ACTIVE  TN 020 0 01 06  MG011
ORIG TN 020 0 01 06  MG011  KEY 0 SCR MARP  CUST 1 DN 1006  TYPE 2616
  VGW TN 020 0 04 01
  MEDIA ENDPOINT IP: 10.10.1.17  PORT: 5202
TERM TN 020 1 01 09  MG012  KEY 0 SCR MARP  CUST 1 DN 1109  TYPE 3904
  VGW TN 020 1 03 01
  MEDIA ENDPOINT IP: 10.10.1.50  PORT: 5202
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 10 ms  VAD OFF
DIAL DN 11092
MAIN_PM  ESTD
TALKSLOT  ORIG  7   TERM  71
EES_DATA:
NONE
QUEU  NONE
CALL ID 0 24997
```

Alphabetical list of Call Trace outputs

This section provides definitions of the data output by the various call trace commands.

A time stamp is added to Call Trace output. The following information is added below the time stamp as necessary:

- A digital telephone with no active call register shows: IDLE TN l s c u
- A locked out telephone or digital trunk shows: LOCKOUT TN l s c u (or l ch)
- A disabled telephone or digital trunk shows: DSBL TN l s c u (or l ch)
- A telephone or digital trunk that is in maintenance busy state shows: MSBY TN l s c u (or l ch) MSBY TN l s c u (or l ch) MARP shows if the TN is a MARP TN
  - ACTIVE = the call/key is active
  - AUX_NARS = Network Automatic Route Selection (NARS) data to follow
  - AUX_PM = auxiliary progress mark may be any of the following depending on the MAIN_PM:
    - ABSORBING = performing digit manipulation on the call

  - AWAIT ANI = waiting for Automatic Number Identification information
  - AWAITREPLY = CPU is waiting for a response during a dial sequence
  - BSYG = busy tone to originator
  - CDR-CALLRECORD = CPU is outputting a CDR record
  - CDR-TIMING = CPU is computing a CDR record
  - COMPLETE = dialing is complete
  - DNTRANS = DN translation to TN in progress
  - FAREND-OFF =
  - NARS = call is a network call
  - NOOUTPULS = outpulsing complete, originator receiving ringback
  - OUTPULSING = outpulsing digits related to the call
  - OVLF = resources not available, returning overflow to originator
  - PAUSING = timed pause in a trunk call dialing sequence
  - SPEEDCALL = performing speed call
  - TEMPPATH = software timing, occurs when outpulsing digits on trunks
  - TOLLCHECK = checking access restrictions for the call
  - USCR = User Selectable Call Redirection programming, receiving dial tone
  - USCR_DIAL = USCR programming

- AUX_RGAT_PM = Ring Again over trunk information
- BEARER CAP = bearer capability, such as voice, 64K clear, 64K restricted and 56K
- BUSY = unit or DN is busy
- CALL REF # = PRI call reference number assigned by the system
- CALL STATE = specifies the PRI call as active or inactive
- CALLED NO = PRI dialed number
- CALLING N0 = PRI home location code and DN of originating party
- CONF = conference call
- COS_ORIG, COS_TERM = class of service restrictions for originating and terminating party. Possible values are:
  - UNR = Unrestricted
  - TLD = Toll Denied
  - SRE = Semi-restricted
  - FRE = Fully Restricted

  - FR1 = Fully Restricted class 1
  - FR2 = Fully Restricted class 2
  - CUN = Conditionally Unrestricted
  - CTD = Conditionally Toll Denied

- CSD = Confree Selectable Display Key
- CUST = Customer Number
- DARK_CONSOLE = the call is being temporarily released by a console. Also outputs three types of recall:
- RLSED = console released the call is getting recall
- FLASH = Flash recall
- CAMP = Camp-On recall
- DIAL DN = the dialed number
- DIAL xxx yy TTR zz = TDS on loop xxx and timeslot yy connected to Digitone Receiver timeslot zz
- DG_MAN xxx FCA_INDEX xxx TOD x = Digit Manipulation Index, Free Area Screening and Time Of Day value
- DIRECT MW_CALL = Message Waiting indication is being given DN = Directory Number
- DSBL = the unit has been disabled
- DST = console destination information to follow
- EMR100 = ACD emergency conference
- EXP_ROUTE = identifies if an expensive route is being used for an ESN call
- EXTENDED LOCAL CALL is printed out if call traces are printed for Extended Local Call
- IDLE = TN or key is idle
- HLD = number of calls On-Hold at the console
- HOLD = call is On-Hold
- KEY = Telephone function key
- LOCKOUT = the unit is in lockout state
- LOOP = attendant console LPK key
- MAIN_PM = this is the main progress mark which identifies the state of the call, possible values are listed below: (See also AUX_PM)
  - BUSY = originator is receiving busy tone
  - CDR = CPU is processing Call Detail Recording records

- DELAY DIAL = CPU is in a timing sequence while establishing a delay dial start trunk call
- DIAL = one or more digits have been dialed, system requires more digits
- ESTD = call is established between the originating and terminating party
- HALFDISC = Trunk with answer supervision has not received a disconnect signal from the far-end during trunk idling
- READY = CPU is ready to process a function for the originating TN
- REOR = originator is receiving intercept treatment
- RING = originator is receiving ringback tone
- WAIT = dial tone waiting queue
- WINKON = CPU is in a timing sequence while establishing a wink start trunk call
- MARP = indicates the TN is Multiple Appearance Redirection Prime
- MBSY = unit is in maintenance busy state
- NARS_PM = NARS call progress mark
- NEW_RLIST_INDEX NWQ_RLIST_ENTRY = network queue route list index and route list entry
- NCOS_ORIG, NCOS_TERM = Network Class of Service for originating and terminating party
- OHQ/CBQ = call is in the Off-Hook queue or Callback queue
- OSN = On-Site Notification key
- PRIOITY NWQ_EXT_ROUTE = the priority in the queue and extended route queuing
- PTY SLOT = TDS priority timeslot; reserved by the CPU while a user is receiving tones (this timeslot may be required by the CPU to further process the call). Normally PTY SLOT is the same timeslot as SLOT.
- QUEU = a call may be in one of the following CPU timing queues:
- 128 = 128 ms timing queue 2S = 2 second timing queue CAD = cadence CDR = Call Detail Recording processing queue DIAL = dialing queue IDLE = idle queue NONE = call is not in a timing queue RING = ringing queue
- RCVR xx SET yy = timeslot to the Digitone Receiver (xx) and the telephone (yy)
- RGAT_PM = Ring Again progress mark
- RL_IND xx RL_ENT xx = NARS/BARS route list index and entry number
- SRC = console source information to follow
- SBSY = unit is software busy

- SLOT = the timeslot used by the originator and terminator
- TALKSLOT = identifies the timeslot and junctor (if applicable) used by the originator and terminator
- TDTN = Tone Digit Switch loop and timeslot
- TERM = originating party information, identifies the TN or DN where the call terminates, output depends on type of telephone or console
- TGAR_ORIG, TGAR_TERM = Trunk Group Access Restriction for originating and terminating party
- TTR = Digitone Receiver TN

- TYPE = Type of telephone

Basic commands

DALL	Disable all enhanced trace commands.
DIST n	Disable the enhanced trace operation.
ENTC l s c u t	Enable the enhanced trace command for a TN.
ENTD l ch t	Enable the enhanced trace command for a digital trunk.
FITR	Get information about the enhanced trace function.
GOTR	Begin enhanced trace commands. This command starts the trace operation specified with the ENTC and ENTD commands.
STPT	Stop the enhanced trace command.
TRAC c acod	List route number, type and status of each trunk for customer c
TRAC c dn	Trace calls for customer c Directory Number or Local Steering Code dn
TRAC c r m	Trace calls, customer c, route r, member m
TRAC l s c DSLx	Trace calls on Digital Subscriber Loop x (0-7)
TRAC l s c u	Trace calls associated with this unit
TRAC l s c u k	Trace calls associated with key k on specified unit
TRAC x yyyy	Trace using customer number as DN
TRAC xx...xx DEV	Print auxiliary data
TRAC zzzz	Trace using TN of the set to be traced
TRAD loop ch	Trace DTI or DLI calls, channel ch of loop
TRAT c a	Trace calls, attendant a of customer c

TRAT c a k	Trace calls associated with key k of attendant console a for customer c
TRAT l s c u	Trace attendant calls, this unit
TRAT l s c u k	Trace attendant calls on key k
TRAT xx...xx DEV	Print auxiliary data
TRCR l s cu	Trace rejected calls associated with this unit.
TRCR l ch	Trace rejected calls associated with this unit.
TRCR 1	Trace rejected calls associated with any unit.
TRCR 0	Cancel trace.
TRIP <ip address>	Trace IP

Small Systems, CS 1000S, MG 1000B, and MG 1000T commands

On a Small Systems, CS 1000S, MG 1000B, and MG 1000T, some loop-level commands are replaced with slot-level commands. Valid commands for these systems are shown here:

TRAC c acod	List route number, type and status of each trunk under customer c
TRAC c dn	Trace calls for customer c Directory Number or Local Steering Code dn
TRAC c r m	Trace calls for customer c, route r, member m
TRAD c ch	Trace digital calls, channel ch of card c
TRAD loop ch	Trace DTI calls, channel ch of loop
TRAK c u	Trace calls associated with this unit
TRAK c u k	Trace calls associated with key k on the specified unit
TRAO c u	Trace attendant calls, this unit
TRAO c u k	Trace attendant calls on key k of unit
TRAO xx...xx DEV	Print auxiliary data
TRAT c a	Trace calls for attendant a of customer c
TRAT c a k	Trace calls associated with key k of attendant console a for customer c
TRCR cu	Trace rejected calls associated with this unit.
TRCR l ch	Trace rejected calls associated with this unit.

TRCR 1	Trace rejected calls associated with any unit.
TRCR 0	Cancel trace.
TRDT xx...xx	Trace the TNs of a call using 4 to 7 consective digits xx...xx.

Alphabetical list of commands

Command	Description	Pack/Rel
DALL	Disable all enhanced trace commands. This command disables all trace commands enabled with ENTC or ENTD command. You must stop the trace with the STPT command before disabling all the commands with DALL.	basic-19
DIST n	Disable the enhanced trace operation. This command disables the trace command enabled with ENTC or ENTD command. This command is used once a trace command is started then stopped. Where: n = the entry number (as seen with the FITR command)	basic-19
ENTC l s c u t	Enable the enhanced trace command for a TN. This command enables the trace capability for the TN specified. Note that this command does not start the trace immediately. Use the GOTR command to begin the trace operation. Where: l = loop, s = shelf, c = card, u = unit and t = the length of time the trace command operates. The format for the trace command duration (t) is HHMM, where HH = hours (0-23)and MM = minutes (0-59). For example, for a duration of 5 minutes, t = 0005; for 1 hour, t = 0100 The time duration must be at least 1 minute, and no more than 23 hours.	basic-19
ENTD l ch t	Enable the enhanced trace command for a digital trunk. This command enables the trace capability for the TN specified. Note that this command does not start the trace immediately. Use the GOTR command to begin the trace operation. Where: l = loop, s = shelf, c = card, u = unit and t = the length of time the trace command operates.	basic-19

Command	Description	Pack/Rel
	The format for the trace command duration (t) is HHMM, where HH = hours (0-23)and MM = minutes (0-59). For example, for a duration of 5 minutes, t = 0005; for 1 hour, t = 0100. The time duration must be at least 1 minute, and no more than 23 hours.	

FITR	Get information about the enhanced trace function. This command queries the TNs or Digital trunks being traced with the ENTC and ENTD commands.
	The output is shown as follows:
	`ENTRY TN or TRUNK TIME STATUS`
	For example:
	`1 01 0 01 01 0030 OFF`
	`2 015 04 1200 OFF`
		basic-19

GOTR	Begin enhanced trace commands. This command starts the trace operation specified with the ENTC and ENTD commands.	basic-19
STPT	Stop the enhanced trace command. This command stops the enhanced trace operation specified with the ENTC and ENTD commands. This can be used at any time during the trace operation. This does not disable the commands; they can be restarted with the GOTR command. When they are restarted, the duration timer is reset. For example: the timer is set at 30 minutes, but the trace is stopped after 2 minutes. When the trace is restarted (GOTR) the timer is set to 30 minutes.	basic-19
TRAC c acod	List route number, type and status of each trunk for customer c.	basic-1
TRAC c dn	Trace calls for customer c Directory Number or Local Steering Code dn.	basic-1
	With release 4.5 Active Call Failover status is output as: ACF STATUS <status> TMR <timer> ORIG <orig_state> TERM <term_state>, where status is: - UNREG for unregistered calls - HREG for half-registered calls	basic-4.50

Command	Description	Pack/Rel
	- HREB for half-rebuilt calls - REB for rebuilt calls - PREB for partially-rebuilt call where timer is: - an integer value if the timer exists for the call - N/A if there is no Call Server ACF timer attached where orig_state is: - UNREGISTERED for unregistered calls - REGISTERED for registered calls where term_state is: - UNREGISTERED for unregistered calls - REGISTERED for registered calls	basic-4.50
	Note: LD 32 shows sample outputs for IP phones involved in unregistered and partial-rebuilt calls	

	Trace command:
	`.trac 0 8100`
	Output:
	`ACTIVE TN 081 0 00 00 V PHYSICAL TN 003 0 00 04`
	`ORIG 008 0 00 00 0 SCR MARP 0 5500 2616`
	`TERM 081 0 00 00 V PHYSICAL TN 000 0 00 00 0 SCR MARP`
	`RING ON 0`
	`8100 I2004`
	`DIAL DN 8100`
	`MAIN_PM ESTD`
	`TALKSLOT ORIG 17 TERM 14`
	`EES_DATA:`
	`NONE`
	`QUEU NONE`
	`CALL ID 0 197`
	`ACF STATUS UNREG TMR 110 ORIG UNREGISTERED TERM`
	`UNREGISTERED`	

TRAC c r m	Trace calls, customer c, route r, member m.	basic-1
TRAC l s c DSLx	Trace calls on Digital Subscriber Loop x (0-7).	bri-18

Command	Description	Pack/Rel
TRAC l s c u	Trace calls associated with this unit. If a trace is performed on a DTR, an error message is output.	basic-1
TRAC l s c u k	Trace call associated with key k on specified unit.	basic-1
TRAC x yyyy	Trace using customer number as DN, where: • x = customer number of the set to be traced • yyyy = DN of the key to be traced.	nxcc-22
TRAC xx...xx DEV	Print the auxiliary data related to the call for Network Alternate Route Selection (NARS), Basic Alternate Route Selection (BARS), Coordinated Dialing Plan (CDP) or Ring Again (RGA), where equipped, as well as the normal data for command xx...xx. Command xx...xx can be any of the TRAC commands. When TYP E is output, E = extended route (not expensive).	nxcc-22
TRAC zzzz	Trace using TN of the set to be traced, where: zzzz = TN of the set to be traced.	nxcc-22
TRAD loop ch	Trace DTI or DLI calls, channel ch of specified loop.	basic-1
TRAD c ch	Trace digital calls, channel ch of card c. (Small System, CS 1000S, MG 1000B,MG 1000T).	
TRAK c u	Trace calls associated with this unit. (Small System, CS 1000S, MG 1000B,MG 1000T).	basic-1
TRAK c u k	Trace calls associated with key k on the specified unit. (Small System, CS 1000S, MG 1000B,MG 1000T).	basic-1
TRAO c u	Trace attendant calls, this unit. (Small System, CS 1000S, MG 1000B,MG 1000T).	basic-1
TRAO c u k	Trace attendant calls on key k of unit. (Small System, CS 1000S, MG 1000B,MG 1000T).	basic-1
TRAO xx...xx DEV		basic-1

Command	Description	Pack/Rel
	Print auxiliary data. (Small System, CS 1000S, MG 1000B,MG 1000T).	
TRAT c a	Trace calls for customer c, attendant a.	basic-1
TRAT c a k	Trace calls associated with key k of attendant console a for customer c.	basic-1
TRAT l s c u	Trace attendant calls, this unit.	basic-1
TRAT l s c u k		
	Trace attendant calls on key k.	basic-1
TRAT xx...xx DEV		basic-1
	Print auxiliary data. Print the auxiliary data related to the call for Network Alternate Route Selection (NARS), Basic Alternate Route Selection (BARS), Coordinated Dialing Plan (CDP) or Ring Again (RGA), where equipped, as well as the normal data for command xx...xx. Command xx...xx can be one of the TRAT commands.	
TRCR cu	Trace rejected calls associated with this unit.	basic-4.50
TRCR l s c u	Trace rejected calls associated with this unit.	basic-4.50
TRCR l ch	Trace rejected calls associated with this unit.	basic-4.50
TRCR 1	Trace rejected calls associated with any unit.	basic-7.00
TRCR 0	Cancel trace.	basic-4.50
TRDT xx...xx	Trace the TNs of a call using 4 to 7 consective digits xx...xx.	basic-7.50
TRIP <ip address>	Trace IP	basic-5.00

Chapter 29: LD 92: Automatic Trunk Maintenance

The Automatic Trunk Maintenance (ATM) program tests TIE, CSA, WATS, FEX, DID, and COT trunk routes automatically each day at times scheduled in the ATM schedule block. This program also allows the manual testing of trunks.

Some loop-level commands are not valid on Small Systems and CS 1000S systems, and have been replaced with card-level commands.

The ATMC command is not supported for 2.0 Mb/s DTI due to the absence of tone detectors for Small System in IPE.

Basic commands

On Small Systems and Avaya Communication Server 1000S systems, some loop-level commands are replaced with card-level commands.

ATMC l ch	Test DTI channel ch on loop
ATMC l ch l ch	Test specified DTI channel, with reference trunk
ATMR c r	Test customer c route r
ATMR c r m	Test customer c route r with reference trunk member m
ATMU c u	Test specified unit. (Small System)
ATMU c u c u	Test specified unit, with reference trunk. (Small System)
ATMU l s c u	Test specified unit
ATMU l s c u l s c u	Test specified unit, with reference trunk
CLRR c r	Clear "ring no answer" count on route r for customer c
CLRU c u	Clear "ring no answer" count on specified trunk unit. (Small System)
CLRU l s c u	Clear "ring no answer" count on specified trunk unit
CMAJ	Clear major alarm and reset power fail transfer
END	Terminate test in progress

PRTR c r	Get "ring no answer" count for all members on route r for customer c.
PRTU c u	Get "ring no answer" count on specified unit. (Small System)
PRTU l s c u	Get "ring no answer" count on specified unit.
PSCD l ch	Print the current value of the SPC Calls to the Data Interface Counter
RSCD l ch (n)	Restart the Semi Permanent Connections (SPC) calls to Data Interface counter
SSCD l ch	Stop the SPC calls to Data Interface to be performed

Alphabetical list of commands

Command	Description	Pack/Rel
ATMC l ch	Test DTI channel ch on loop.	atm-7
ATMC l ch l ch	Test the specified DTI channel (loop and channel of the first field) with the reference trunk (loop and channel of the second field).	atm-7
ATMR c r	Test route r of cu7stomer c. Accepts ADM Route numbers. When an ADM Route is entered, member numbers cannot be entered.	atm-7
ATMR c r m	Test route r of customer c with reference trunk member m.	atm-7
ATMU c u	Test specified unit. (Small System)	atm-15
ATMU c u c u	Test specified unit, with reference trunk. (Small System)	atm-15
ATMU l s c u	Test specified unit. If the unit specified is an ADM trunk unit, no reference information can be entered.	atm-7
ATMU l s c u l s c u	Test the specified unit (l s c u of the first field) using the reference trunk (l s c u of the second field). If the unit specified is an ADM trunk unit, no reference information (l s c u) can be entered.	atm-7

Command	Description	Pack/Rel
CLRR c r	Clear "ring no answer" count on route r for customer c. Clears the "ring no answer" count for every trunk member in the ADM Route specified.	atm-7
CLRU c u	Clear "ring no answer" count on specified trunk unit. (Small System)	atm-15
CLRU l s c u	Clear "ring no answer" count on specified trunk unit.	atm-7
CMAJ	Clear major alarm, reset power fail transfer and clear power fault alarm.	atm-7
END	Terminate test in progress. This command can be entered at any time.	atm-7
PRTR c r	Get "ring no answer" count for all members on route r for customer c.	atm-7
PRTU c u	Get "ring no answer" count on specified unit. (Small System)	atm-15
PRTU l s c u	Get "ring no answer" count on specified unit.	atm-7
PSCD l ch	Print the current value of the SPC Calls to the Data Interface Counter.	ispc-22
RSCD l ch (n)	Restart the Semi Permanent Connections (SPC) calls to Data Interface counter, where: • l = Phantom loop of an SPC link • ch = Phantom TN of an SPC link. The RSCD command resets the current counter used to identify the number of calls performed by the system to the Data Interface when an SPC link is configured to convey D-channel signaling and the SPC link is identified as being the SLAVE side. The optional parameter (n) is used to identify the maximum number of calls to the Data Interface before the process automatically stops. When no value has been provided to the parameter (n), up to 40 calls to the Data Interface are performed before this process is automatically stopped. When the value provided to the parameter (n) is zero, it has to stop the process which automatically calls the associated Data Interface.	ispc-22

Command	Description	Pack/Rel
SSCD l ch	Stop the SPC calls to Data Interface to be performed.	ispc-22

Chapter 30: LD 96: D-channel Diagnostic

LD 96 is used to test, maintain, and trace D-channel links and the QPC757 or NT6D11AB D-channel Interface (DCHI) card.

D-channels can also reside on Multi-purpose Serial Data Link (MSDL) cards. A set of LD 96 commands are provided to support MSDL cards. The MSDL commands listed in LD 48 can also be used in LD 96.

Monitoring

Selective D-channel message monitoring is used to analyze the Layer 3 protocol messages traveling between the near and far-end D-channels:

- the D-channel
- the B- or ISL channel
- the message types for a specific feature
- the message types for a specific DN
- any specific message

The following sections describe the various command formats.

Note:
During high traffic some of the monitored messages may be lost.

Note:
For the D-channel monitor messages to be displayed, the system terminal must have USER defined as MTC in LD 17.

D-channels

All message types, features and channels associated with a particular D-channel can be monitored for multiple D-channels for both incoming and outgoing messages.

Message output can be routed to the terminal or to a log file on the Call Server. The location of the log file is: /e/trace/dch.log. The log file holds 4000 records and can be downloaded from the Call Server by FTP.

The LD 96 commands to enable or disable monitoring of all incoming or outgoing messages on a D-channel are:

ENL MSGI x – enable monitoring of incoming messages ENL MSGO x – enable monitoring of outgoing messages DIS MSGI x – disable monitoring of incoming messages DIS MSGO x – disable monitoring of outgoing messages

Where x is the DCHI or MSDL port address (I/O address). For example, to enable monitoring of incoming messages on D-channel 5, enter:

ENL MSGI 5

The output includes all messages, features and channels for D-channel 5.

B-channels and ISL channels

You can monitor up to 5 ISL or B-channels, for each direction. If there is no specific channel selected, all channels are monitored. The commands follow:

For B-channels on large systems:

ENL MSGI x CH loop channel ENL MSGO x CH loop channel DIS MSGI x CH loop channel DIS MSGO x CH loop channel

For B-channels on Small Systems, CS 1000S, and MG 1000T systems:

ENL MSGI x CH card channel ENL MSGO x CH card channel DIS MSGI x CH card channel DIS MSGO x CH card channel

For ISL channels on large systems:

ENL MSGI x CH l s c u ENL MSGO x CH l s c u DIS MSGI x CH l s c u DIS MSGO x CH l s c u

For ISL channels on Small Systems and CS 1000S systems:

ENL MSGI x CH c u ENL MSGO x CH c u DIS MSGI x CH c u DIS MSGO x CH c u

- ENL = enable monitoring
- DIS = disable monitoring
- MSGI = incoming messages
- MSGO = outgoing messages

ISDN features

You can select specific ISDN applications, such as Network Ring Again, for message monitoring. Only one or all ISDN applications can be monitored per D-channel at one time.

The LD 96 commands are listed below, where x is the D-channel (DCHI or MSDL) port number.

ENL MSGI x FEAT feature ENL MSGO x FEAT feature DIS MSGI x FEAT feature DIS MSGO x FEAT feature

Where "feature" can be:

NCT = Network Call Trace NRAG = Network Ring Again NACD = Network Automatic Call Distribution TRO = Trunk Optimization NMS = Network Message Services OHQ = Offhook Queuing RCFW = Network Remote Call Forward NRPA = Network Radio Paging NITC = Network Intercom TAT = Trunk Anti-Tromboning

D-channel DN tracing

The D-channel call trace feature allows the recording of all relevant D-channel messages for incoming/outgoing calls on a particular Directory Number (DN). It aids a craftsperson in troubleshooting problems for calls involving DCHs.

For example, if a problem arose when making an outgoing DCH call from extension 4567, then the craftsperson would login to the Call Server associated with the DN, load overlay 96 and use the DCT (DCH Call Trace) command for tracing the call on DN 4567 (ie. DCT 4567). When the call is tried again, the DCH call trace output shows any DCH messages associated with the call. If no DCH messages are generated, then the craftsperson can assume that the problem is within the switch (i.e. routing configuration or user mis-operation). If DCH messages are generated, then the craftsperson can inspect the messages for clues about why the call is failing.

It is not expected that the feature to enable/disable incoming/outgoing DCH messages (ENL/DIS MSGO/I commands) would be used at the same time as the DCT feature. Both features are independent of each other. If both features are turned on, then any DCH message captured by either feature is recorded. However, any given DCH message is only recorded once.

Any DCH messages caught by the DCT monitor are recorded in the level format specified by the SET MSGO/I <dch> MON <level> command. The DCT feature has no effect on the format of the messages that are recorded. Any DCH messages are recorded in the usual way (ie. to a TTY and/or log file. The DCT feature has no effect on where the messages are recorded. The DCT monitor data does not survive system cold/warm start. When the system initializes, all DCT data is cleared and the threshold for the number of DCH messages per minute is reset to the default value of 30.

Message types

You can select specific types of messages to be monitored on a D-channel. The LD 96 commands are listed below, where x is the D-channel (DCHI or MSDL) port number.

ENL MSGI x MSG msg1 msg2 msg3 ENL MSGO x MSG msg1 msg2 msg3 DIS MSGI x MSG msg1 msg2 msg3 DIS MSGO x MSG msg1 msg2 msg3

Up to three message types (msg1, msg2, msg3) can be entered per command. The default is "ALL", which is all message types except SVC and SVCA. The message types are:

- ALER = alerting
- ALL = all primitives and all messages except SVC and SVCA
- CAPR = call proceeding
- CON = connect
- CONA = connect ack
- DISC = disconnect
- FAC = facility
- FACA = facility ack
- FACR = facility reject
- INFO = information
- NOTF = notify
- PRIM = all primitives (such as release indication)
- PROC = call proceeding
- PROG = progress
- RLS = release
- RLSC = release complete
- RST = restart
- RSTA = restart ack
- STAT = status
- STEN = status enquiry
- STP = setup
- STPA = setup ack
- SVC = service

- SVCA = service ack
- UI = user information

Setting output format levels

There are three levels (0-2) of message decoding. The level determines the format of the data output to the system terminal. To set the output level enter the following:

SET MSGI x MON (0)-2 SET MSGO x MON (0)-2

Level 0 outputs the message as shown below.

DCH x y MSG msgtype REF xxxxxxx CH zzzz TOD hh:mm:ss <more data>

- x = D-channel number
- y = "I" for incoming messages, "O" for outgoing messages
- xxxxxxxx = the call reference number
- zzzz = the loop and channel number (or TN for ISL channels)
- <more data> = additional lines of information, such as:
- CALLED # = called number
- CALLING # = calling number of originator
- CAUSE = reason for action taken (e.g, unassigned number)
- CONNECT # = connected number
- FEAT = feature (such as Network Ring Again)
- NUM PLAN = Numbering plan used (such as private)
- PROGRESS = call progress description
- REDIR REASON = reason the call was re-directed
- REDN # = call redirection number
- STATE = call state
- STATUS = channel status
- TYPE = type of channel

Level 1 outputs the raw data.

The format is:

DCH x y MSG msgtype REF xxxxxxxx TN zzzzzz CH# x CK x <more data in hexadecimal>

Level 2 output identifies the individual Information Elements (IE) in the messages and their hexadecimal values. The possible IEs are:

- BCAP = bearer capability
- CAST = call state
- CHGA = charge advice
- CHID = channel ID
- CHST = change status
- CLED = called number
- CLES = called party subaddress
- CLNG = calling number
- CLNS = calling party subaddress
- CNS5 = codeset 5 connected number subaddress
- CON# = connect number
- CON5 = codeset 5 connected number
- CSE = cause
- DES6 = codeset 6 Destination IE
- DISP = display
- FAC = facility IE for codeset 0
- FAC6 = codeset 6 facility IE
- FIND = feature Indication
- HLYR = higher layer compatibility
- INFO = information request
- KYPD = keypad
- LLYR = low layer compatibility
- LS5 = locking Shift to codeset 5
- LS6 = locking shift to codeset 6
- LS7 = locking Shift to codeset 7
- NLS5 = codeset 5 non-locking shift
- NLS6 = codeset 6 non-locking shift
- NLSO = non-locking shift to codeset 0
- NOTI = notify indicator
- NSF = network specific facility

- ORG# = originating called number
- ORG6 = codeset 6 Originating IE
- PROG = progress indicator
- RDG6 = codeset 6 redirecting number
- REDG = redirecting number
- REDN = redirection number
- RETR = codeset 6 reason for return
- RSTI = restart indicator
- SHFT = shift
- SIGN = signal
- TACG = codeset 6 TTC advice charge
- TNS = transit network selection
- UNKN = unknown
- UUI = user-user information

Deactivate monitor from a maintenance telephone

Once the system has been tied up or flooded with the monitored messages, it is very difficult, if not impossible, to use LD 96 to disable the monitors. In this case, a maintenance telephone with MTA Class of Service can be used to deactivate the monitor.

To activate or deactivate the monitor from a maintenance telephone, simply dial: SPRE 9913 x 01

- SPRE = special function access code (defined in LD 15)
- 9913 = feature code to activate or deactivate the monitor
- x = 0 to deactivate, 1 to activate
- 01 = DCH monitor ID

Note:
Dial tone is provided if successful.

Note:
Use "RST MON" to reactivate the monitor from LD 96.

Note:
Deactivating the monitor by the maintenance telephone does not disable the monitor, but simply halts the output. If the monitor is deactivated and not disabled using the DIS MSGI

and DIS MSGO commands, then the monitor becomes re-activated after a datadump and sysload.

Get monitor status

To determine the current status of the D-channel monitor, enter the following command, where x is the D-channel (DCHI or MSDL) port number.

STAT MON x

Output format:

***DCH MSGI x LEVEL y ACTV (where, y = format level)

MSG - msg1 msg2. . .

FEAT - feat

CH - loop channel (or l s c u for ISL)

***DCH MSGO x LEVEL y ACTV

MSG - msg1 msg2. . .

FEAT - feat

CH - loop channel (or l s c u for ISL)

If the monitor had been deactivated by the maintenance telephone, INACTV is output instead of ACTV.

Example: Status of D-channel monitor

STAT MON x DCH MON DCH 003: (UIPE) MSGI (LEVEL 1) : DSBL DBGI (LEVEL 1) : DSBL MSGO (LEVEL 2) MSG = PRIM ALER DISC FAC FRNC FJNC INFO MIFO NOTE PROC PROG REJ RLS STP STPR STEN STAT RST RSTR SVC SVCR RSTJ NSM1 NSM2 REGI CH = 003 10 SET = ON DBGO (LEVEL 2) MSG = PRIM ALER DISC FAC FRNC FJNC INFO MIFO NOTF PROC PROG REJ RLS STP STPR STEN STAT RST RSTR SVC SVCR RSTJ NSM1 NSM2 REGI CH = 003 10 SET = ON

Multi-purpose Serial Data Link (MSDL)

The MSDL provides 4 ports for ISDN Primary Rate D-channel (DCH) and Application Module Link (AML).

The MSDL commands are listed below, x is the MSDL device number (defined by prompt DNUM in LD 17).

DIS MSDL x (ALL)—Disable MSDL device ENL MSDL x (FDL, ALL)—Enable MSDL device RST MSDL x—Reset MSDL device STAT MSDL (x) (FULL)—Get MSDL status SLFT MSDL x—Execute a self-test on MSDL device x

These commands are also provided in Input/Output Diagnostic (LD 37) and Link Diagnostic (LD 48).

D-channel Expansion

With the introduction of D-channel Expansion, new software allows the increase of D-channels past sixty-four. Instead of the large system having a maximum of 16 I/O addresses, the new software allows 16 physical I/O addresses (0 - 15) per network group for D-channels defined on MSDL. With this enhancement a response to the system response GROUP is required to inform the system of the desired network group.

Note:
See D-channel Expansion commands on page 332 for a complete description of these commands.

CS 1000S Survivable IP

D-ch commands for the DCHI, DDCH, TMDI, and MSDL are all supported for cards in the MG 1000S.

D-channel commands

The following commands are used to enable, disable, test and get the status of a D-channel. Refer to the LD 96 introduction for details on the use of these commands.

The maintenance commands for the TMDI card have been enhanced. You no longer need to use both Overlay 60 and Overlay 96 for TMDI card and loop maintenance. Only Overlay 96 is required to handle enabling and disabling of TMDI cards and their associated loop.

DIS AUTO x	Disable automatic recovery for DCH x
DIS DCH x	Disable DCH x

DIS MON ALL	Stop printing and logging messages.
DIS MON LOG	Stop logging DCH messages into a log file.
DIS MON TTY	Stop printing DCH messages on the TTY.
DIS MSGI x (options)	Disable the monitoring of incoming messages on D-channel x
DIS MSGI x FEAT CPNW	Disable incoming monitoring for the Network CPNW ISDN messages on D Channel x.
DIS MSGO x (options)	Disable the monitoring of outgoing messages on D-channel x
DIS MSGO x FEAT CPNW	Disable outgoing monitoring for the Network CPNW ISDN messages on D Channel x.
DIS SERV x	Disable service messages on D-channel x
DIS TMDI x (ALL)	Disable TMDI card x
DIS TMD l s c (ALL)	Disable TMDI card
DLIF DCH x	Force download of D channel x (For PRI UIPE application)
ENL AUTO x	Enable automatic recovery for DCH x
ENL DCH x (FDL)	Enable DCH x and attempt to establish the link, and force download to MSDL
ENL MON ALL	Print messages on the TTY and log them into a file.
ENL MON LOG	Prepare to log DCH messages into a log file.
ENL MON TTY	Prepare to print DCH messages on the TTY.
ENL MSGI x (options)	Enable the monitoring of incoming messages on D-channel x
ENL MSGI x FEAT CPNW	Enable incoming monitoring for the Network CPNW ISDN messages on D Channel x.
ENL MSGO x (options)	Enable the monitoring of outgoing messages on D-channel x
ENL MSGO x FEAT CPNW	Enable outgoing monitoring for the Network CPNW ISDN messages on D Channel x.
ENL SERV x	Enable service messages on D-channel x
ENL TMDI x	Enable TMDI card number x.
ENL TMDI x (ALL)	Enable TMDI Card number x and all units.
ENL TMDI x (FDL)	Enable TMDI Card number x and force a download.
ENL TMDI l s c	Enable TMDI card
ENL TMDI l s c (FDL,ALL)	Enable TMDI card and force a download
EST DCH x	Establish multiple frame operation on D-channel x

EST ISPC l ch (N)	Start the data interface establishment process at the ISPC slave side an ISPC link (where "N" = the "number of tries" counter)
FDIS NCAL <DCH#> <conn_ID>	Force disconnect the specified call-independent connection
PLOG DCH x	Print protocol error log on DCH x
RLS DCH x	Release D-channel x
RLS ISPC l ch	Stop the data interface establishment process
RST DCH x	Reset D-channel x, inhibit signaling
RST MON	Reset or reactivate monitoring on D-channels with enabled monitors
RST TMDI x	Reset TMDI card x
RST TMDI l s c	Reset TMDI card
SDCH DCH x	Switch to the standby D-channel x
SET MSGI x MON (0)-2	Set monitor output format level for incoming messages on D-channel x
SET MSGO x MON (0)-2	Set monitor output format level for outgoing messages on D-channel x
SLFT TMDI x	Invoke self test x
SLFT TMDI l s c u	Invoke self test
STAT DCH (x)	Get status of one or all D-channels
STAT ISPC l ch	Get status of data interface establishment process at ISPC slave side ISPC link which has been configured to convey D-channel signaling
STAT NCAL <DCH#>	List all current call-independent connections on a given PRI D-channel.
STAT NCAL <DCH#> <conn_ID>	List information pertaining to a specific call-independent connection
STAT MON (x)	Display the incoming and outgoing monitoring status of one or all D-channels.
STAT SERV (x)	Get the enable/disable status of services messages for one or all D-channels

STAT TMDI (x FULL)	Get TMDI status x
STAT TMDI l s c (FULL)	Get TMDI status
TEST 100 x	Perform interrupt generation test on DCH x
TEST 101 x	Perform loop back mode test on DCH x
TEST 200 x	Perform interrupt handler test on DCH x (not supported on small system)
TEST 201 x	Test interrupt handler-to-link interface path (not supported on small system)

D-channel Expansion commands

Command	System Response	Description
STAT MSDL	GROUP	Display status of all MSDL cards in the system, where: If the answer to the GRP prompt is <CR>, then the status of all MSDL cards is printed. If the answer to the GRP prompt is g, then the status of all MSDL cards occupying the g network group is printed.
STAT MSDL n	GROUP	Display status of the given MSDL card as known to the SL1, where: If the answer to the GRP prompt is <CR>, then the status of the MSDL cards occupying the physical I/O address n in all the network groups is printed. If the answer to the GRP prompt is g, then the status of the MSDL card occupying the physical I/O address n in network group g is printed.
STAT MSDL n full		
	GROUP	Display status of the given MSDL card as known to the SL1 and available in the shared RAM of the MSDL card, where: If the answer to the GRP prompt is <CR>, then the status of the MSDL cards occupying the physical I/O address n in all the network groups is printed. If the answer to the GRP prompt is g, then the status of the MSDL card occupying the physical I/O address n in network group g is printed.
ENL MSDL n	GROUP	Enable the given MSDL card, where: If the answer to the GRP prompt is g, then the MSDL card occupying the physical I/O address n in network group g is enabled.

Command	System Response	Description
ENL MSDL n all	GROUP	Enable MSDL card n and all configured ports, where: If the answer to the GRP prompt is g, then the MSDL card occupying the physical I/O address n in network group g is enabled.
ENL MSDL n FDL		
	GROUP	Force download all the required Loadware to the MSDL card and enable the MSDL card, where: If the answer to the GRP prompt is g, then the MSDL card occupying the physical I/O address n in network group g is enabled.
DIS MSDL n all	GROUP	Disable the given MSDL card. All the configured ports should be in the disable state, otherwise the MSDL card can not be disabled, where: If the answer to the GRP prompt is g, then the MSDL card occupying the physical I/O address n in network group g is disabled.
DIS MSDL n ALL	GROUP	Disable all ports of the MSDL card, and then disable the MSDL card, where: If the answer to the GRP prompt is g, then the MSDL card occupying the physical I/O address n in network group g is disabled.
RST MSDL n	GROUP	This command causes a power-on reset on the MSDL card, where: If the answer to the GRP prompt is g, then the MSDL card occupying the physical I/O address n in network group g is reset.
SLFT MSDL n	GROUP	Power-on reset on the MSDL card, followed by a complete set of self tests, where: If the answer to the GRP prompt is g, then the MSDL card occupying the physical I/O address n in network group g is tested.
ENL MSDL n DBG		
	GROUP	Enable the debugger option for the MSDL card, where: If the answer to the GRP prompt is g, then the debugger option for the MSDL card occupying the physical I/O address n in network group g is enabled.
ENL MSDL n MSGO		

Command	System Response	Description
	GROUP	Enable the outgoing message monitor option for the MSDL card, where: If the answer to the GRP prompt is g, then the outgoing message monitor option for the MSDL card occupying the physical I/O address n in network group g is enabled.
ENL MSDL n MSGI		
	GROUP	Enable the incoming message monitor option for the MSDL card, where: If the answer to the GRP prompt is g, then the incoming message monitor option for the MSDL card occupying the physical I/O address n in network group g is enabled.
ENL MSDL n AUDM		
	GROUP	Enable the msdl auditing for the MSDL card, where: If the answer to the GRP prompt is g, then the msdl auditing for the MSDL card occupying the physical I/O address n in network group g is enabled.
ENL MSDL n FCTL		
	GROUP	Enable flow control for the MSDL card, where: If the answer to the GRP prompt is g, then the flow control option for the MSDL card occupying the physical I/O address n in network group g is enabled.
DIS MSDL n DBG		
	GROUP	Disable the debugger option for the MSDL card, where: If the answer to the GRP prompt is g, then the debugger option for the MSDL card occupying the physical I/O address n in network group g is disabled.
DIS MSDL n MSGO		
	GROUP	Disable the outgoing message monitor option for the MSDL card, where: If the answer to the GRP prompt is g, then the outgoing message monitor option for the MSDL card occupying the physical I/O address n in network group g is disabled.
DIS MSDL n MSGI		
	GROUP	Disable the incoming message monitor option for the MSDL card, where: If the answer to the GRP prompt is g, then the incoming message monitor option for the MSDL card occupying the physical I/O address n in network group g is disabled.

Command	System Response	Description
DIS MSDL n AUDM		
	GROUP	Disable the msdl auditing for the MSDL card, where: If the answer to the GRP prompt is g, then the msdl auditing of the MSDL card occupying the physical I/O address n in network group g is disabled.
DIS MSDL n FCTL		
	GROUP	Disable the flow control for the MSDL card, where: If the answer to the GRP prompt is g, then the flow control option for the MSDL card occupying the physical I/O address n in network group g is disabled.
STAT MSDL n MON		
	GROUP	Display the current message monitoring and debug option for the given MSDL card, where: If the answer to the GRP prompt is g, then the current message monitoring and debug option for the MSDL card occupying the physical I/O address n in network group g is displayed.

Multipurpose Serial Data Link (MSDL) commands

The MSDL commands are listed below, x is the MSDL device number (defined by prompt DNUM in LD 17). These commands are also provided in Input/Output Diagnostic (LD 37) and Link Diagnostic (LD 48).

DIS MSDL x (ALL)	Disable MSDL device x
ENL MSDL x (ALL, FDL)	Enable MSDL device x
RST MSDL x	Reset MSDL device x
SLFT MSDL x	Invoke self-test for MSDL device x
STAT MSDL (x [FULL])	Get MSDL status

Note:
See "Alphabetical List of commands" in LD 48 for a complete description of these commands.

Multipurpose Serial Data Link D-channel commands

The following commands are only available for D-channels on an MSDL port.

DIS LLB x	Disable local loop back mode on MSDL DCH x
DIS RLB x	Disable remote loop back mode on MSDL DCH x
DIS TEST x	Disable TEST mode on MSDL DCH x
DLIF DCH xx FDL	Force download a PRI interface table.
ENL LLB x	Enable local loop back mode on MSDL DCH x
ENL RLB x	Enable remote loop back mode on MSDL DCH x
ENL TEST x	Enable TEST mode on MSDL DCH x
MAP DCH x	Get physical address and switch settings for D-channels
PCON DCH x	Print configuration parameters on MSDL DCH x
PMES DCH x	Print incoming layer 3 messages on MSDL DCH x
PTRF DCH x	Print traffic report on MSDL DCH x
PTRF DCH x	Print traffic report on MSDL DCH x
TEST LLB x	Start local loop back test on MSDL DCH x
TEST RLB x	Start remote loop back test on MSDL DCH x

D-channel call trace commands

All LD 96 DCT commands and variants are listed below.

DCT xxxxxxxx	Set the monitor digits (part or all of a DN) for trace operation .
DCT on/off	Turn the DCT monitor on and off.
DCT I xxxxxxxx	Set several occurrences of monitor digits (part or all of multiple DNs) for trace operation.
DCT > n	Change the DCT monitor message threshold.
DCT clr	Clear all DCT monitor settings.

DCT I xxxxxxxx <NPI> <TON> <MsgRecv> <MsgSend>	Specify specific types of calls for monitoring.
DCT dch n	Specify the DCHs to monitor.
DCT dch clr	Remove monitoring for all DCHs.
DCT	Display DCT settings.
DCT help/?	Display DCT commands syntax.

Important:
When monitoring digits with three or fewer digits, only the DCH message with a match is recorded (not any associated messages). This prevents excessive messaging.

Outgoing messages

Table 16: Outgoing messages on page 337 indicates the message mnemonics for outgoing messages for UIPE proprietary and Q.931 messages.

Table 16: Outgoing messages

Message Mnemonic	UIPE Proprietary	Q.931 Messages	Support on Q.931
ALER	CC_ALERT_REQUEST	ALERTING	P
DISC	CC_DISCONNECT_REQUEST	DISCONNECT	P
FAC	CCC_FAC_REQUEST	FACILITY	P
FRNC	CC_FAC_REG_NULL_CRF	FACILITY	P
FJNC	CC_FACREJ_REQ_NULL_CRF	FACILITY REJECT	P
INFO	CC_INFORMATION_REQUEST	INFORMATION	P
MIFO	CC_MORE_INFO_REQUEST	SETUP ACK	P
NOTF	CC_NOTIFY_REQUEST	NOTIFY	P
PROC	CC_PROCEEDING_REQUEST	CALL PROCEEDING	P
PROG	CC_PROGRESS_REQUEST	PROGRESS	P
REJ	CC_REJECT_REQUEST	RELEASE	X
		COMPLETE	
RLS	CC_RELEASE_RESPONSE	RELEASE	P

Message Mnemonic	UIPE Proprietary	Q.931 Messages	Support on Q.931
RLSR	CC_RELEASE_RESPONSE		
STP	CC_SETUP_REQUEST	SETUP	P
STPR	CC_SETUP_RESPONSE	CONNECT	P
STEN	CC_STATUS_ENQ_REQUEST	STATUS ENQUIRY	P
STAT	CC_STATUS_REQUEST	STATUS	P
RST	CC_RESTART_REQUEST	RESTART	X
RSTR	CC_RESTART_RESPONSE	RESTART ACK	X
SVC	SERVICE MESSAGES	SERVICE	P
SVCR	SERVICE RESPONSE	SERVICE	
		RESPONSE	P
RSTJ	CC_RESTART_REJECT	RESTART REJECT	X

Incoming messages

Table 17: Incoming messages on page 338 indicates the message mnemonics for incoming messages for UIPE proprietary and Q.931 messages.

Table 17: Incoming messages

Message Mnemonic	UIPE Proprietary	Q.931 Messages	Support on Q.931
ALER	CC_ALERT_INDICATION	ALERTING	P
DISC	CC_DISCONNECT_INDICATION	DISCONNECT	P
FAC	CCC_FAC_INDICATION	FACILITY	P
FIDC	CC_FAC_IND_NULL_CRF	FACILITY	P
FJDC	CC_FACREJ_IND_NULL_CRF	FACILITY REJECT	P
INFO	CC_INFORMATION_INDICATION	INFORMATION	P
MIFO	CC_MORE_INFO_INDICATION	SETUP ACK	P
NOTF	CC_NOTIFY_INDICATION	NOTIFY	P
PROC	CC_PROCEEDING_INDICATION	CALL PROCEEDING	P

Message Mnemonic	UIPE Proprietary	Q.931 Messages	Support on Q.931
PROG	CC_PROGRESS_INDICATION	PROGRESS	P
RLSC	CC_RELEASE_CONFIRMATIO N	RELEASE	X
		COMPLETE	
RLS	CC_RELEASE_INDICATION	RELEASE	P
REJ	CC_REJECT_INDICATION	RELEASE	
		COMPLETE	P
STP	CC_SETUP_INDICATION	SETUP	P
STPC	CC_SETUP_CONFIRMATION	CONNECT	P
STEN	CC_STATUS_ENQ_INDICATIO N	STATUS ENQUIRY	P
STAT	CC_STATUS_INDICATION	STATUS	P
RST	CC_RESTART_INDICATION	RESTART	X
RSTC	CC_RESTART_CONFIRMATIO N	RESTART ACK	X
SVC	SERVICE MESSAGES	SERVICE	P
SVCR	SERVICE RESPONSE	SERVICE	
		RESPONSE	P

Alphabetical list of commands

Command	Description	Pack/Rel
DCT	Display DCT settings.	basic-6.00
DCT clr	Clears all DCT settings or resets them to their default value. For example, enter "DCT clr" to clear all previously entered DCT command settings and reset the DCH message per minute threshold value to 30 (default).	basic-6.00
DCT help | ?	Display command syntax. You can type the word "help" or enter a "?"; both result in the same output.	basic-6.00
DCT dch n	Configure the D-channels to monitor, where n = D-channel number.	basic-6.00

Command	Description	Pack/Rel
	• Up to 10 D-channels can be monitored. For example, to monitor D-channels 4, 8, 22, and 28, enter DCT dch 4 8 22 28. • Precede a D-channel number with "X" to remove monitoring on that D-channel. For example, enter DCT dch X4 to remove monitoring on D-channel 4. **Note:** All D-channels are monitored by default.	
DCT x...x	Configure a directory number (DN) or portion thereof, for DCT monitoring. Where x...x =: • part or all of an 8-digit DN A minimum of 2, or a maximum of 8, digits can be entered. For example, to monitor for a DN 3331101, enter DCT 3331101. • 0 Clears the previous DCT x...x entry. For example, to clear the entry to monitor 3331101, enter DCT 0. **Note:** There is no need to turn on the DCT monitor before entering this DCT command. The DCT monitor turns on automatically when this command is entered.	basic-6.00
DCT I x...x	Configure multiple directory numbers (DN) or portions thereof, for DCT monitoring. To configure multiple directory numbers (DNs) or portions thereof, an index is required. Where: • I = index number from 1 to 5 • x...x = part or all of an 8 digit DN A minimum of 2, or a maximum of 8, digits can be entered. For example, to monitor DNs 345654 and 67893, enter DCT 1 345654 followed by DCT 2 67893. Messages for DN 345654 are logged in index 1 and messages for DN 67893 are logged in index 2. If a DN is not entered after the index number, the DN number associated with the specified index is cleared. For example, enter DCT 2 to clear the 67893 DN from index 2.	basic-6.00

Command	Description	Pack/Rel
DCT I x...x <NPI> <TON> <MsgRecv> <MsgSend>	Configure specific types of calls to be monitored for the identified DN or portion thereof. Where: • I = index number from 1 to 5 • x...x = part or all of an 8 digit DN A minimum of 2, or a maximum of 8, digits can be entered. • <NPI> = Numbering Plan Indicator Values: - (0) = any number - 1 = Unknown number - 2 = ISDN(E.164) - 3 = Private - 4 = E.163 - 5 = Telex - 6 = Data - 7 = National standard • <TON> = Type of Number Values: - (0) = any type - 1 = Unknown type - 2 = International - 3 = National - 4 = Network Specific - 5 = Subscriber - 6 = Level 1 Regional - 7 = Level 0 Regional • <MsgRecv> = turn on monitoring for incoming messages Values: - (Yes) = monitor incoming DCH messages - No = don't monitor incoming DCH messages • <MsgSend> = turn on monitoring for outgoing messages Values: - (Yes) = monitor outgoing DCH messages	basic-6.00

Command	Description	Pack/Rel
	- No = don't monitor outgoing DCH messages For example, to monitor for international numbers containing 5678 on received incoming DCH messages using a private numbering plan, enter "DCT 1 5678 3 2 on off". To monitor for any type of number containing 56798 on outgoing DCH messages using a Telex numbering plan, enter "DCT 2 56798 5 0 off on". To monitor for unknown numbers in any DCH messages using a private data plan, enter "DCT 3 all 6 1 on on". Command settings override any previously issued command settings. For example, if command "DCT 1 5678 3 2 on off" is issued, followed by command "DCT 1 5908 3 2 off on", settings configured during the first command (5678 3 2 on off) are cleared and replaced by the settings configured for the second command (5908 3 2 off on). Duplicate settings with different indexes are allowed. For example, the following 2 commands can be issued: "DCT 1 5678 3 2 on off" and "DCT 2 5678 3 2 on off" to capture DCH messages for DN 5678 in indexes 1 and 2. This does not cause duplicate DCH messages to be recorded, only one set of messages is recorded. **Note:** Only those D-channels configured in the "DCT dch" command are monitored.	
DCT > n	Set the maximum number of DCH messages that can be recorded per minute for a DCT trace, where n = a number from 1 to 60. Default setting is 30 messages per minute. For example, to turn off DCT tracing when the number of recorded DCH messages exceeds 45 per minute, enter DCT > 45	basic-6.00
DCT <on> <off>	Activates or deactivates the recording of D-channel messages. **Note:** No DCT trace data is cleared.	basic-6.00
DIS AUTO x	Disable automatic recovery for DCH x	pra-13
DIS DCH x	Disable DCH x. This changes the status of the DCH to DSBL and the status of the D-channel to DCH RST (reset).	pra-18

Command	Description	Pack/Rel
DIS LLB x	Disable local loop back mode on MSDL DCH x. See "ENL TEST" command for details.	msdl-18
DIS MON ALL	Stop printing and logging messages.	pra-5.00
DIS MON LOG	Stop logging DCH messages into a log file.	pra-5.00
DIS MON TTY	Stop printing DCH messages on the TTY.	pra-5.00
DIS MSGI x (options)	Disable the monitoring of all incoming messages from D-channel x. The available options are: • `CH loop channel:` disable incoming messages on B-channel loop channel (Large Systems) • `CH card channel :` disable incoming messages on B-channel card channel (Small Systems, CS 1000S, and MG 1000T systems) • `CH l s c u:` disable incoming messages on ISL-channel loop shelf card unit (Large Systems) • `CH c u :` disable incoming messages on ISL-channel card unit (Small Systems, CS 1000S, and MG 1000T systems) • `FEAT feature:` disable incoming messages for a PRI feature • `MSG msg1 msg2 msg3:` disable incoming message types Refer to the LD 96 introduction for details.	pra-17
DIS MSGI <dch> DEBG CH <loop><channel>	Disable the debugging of all monitored incoming messages from D-channel card. A maximum of 5 channels are monitored at a time. Only one channel number can be entered in one command.	basic-3.0
DIS MSGI <dch> DEBG MSG msg1 msg2 msg3	Disable the debugging of all monitored incoming messages from D-channel. This command can be entered more than once. Only 3 message mnemonics can be given in one command.	basic-3.0

Command	Description	Pack/Rel
DIS MSGI <dch> DEBG SET		basic-3.0
	Disable debug SET on all incoming messages from D-channel. This set-based filtering is enhanced for UIPE proprietary messages.	
DIS MSGI x FEAT CPNW		basic-21
	Disable incoming monitoring for the Network CPNW ISDN messages on D Channel x.	
DIS MSGO x (options)		
	Disable the monitoring of outgoing messages from D-channel x. Refer to DIS MSGI x (options) for the list of options.	pra-17
DIS MSGO <dch> DEBG CH <loop><channel>		basic-3.0
	Disable the debugging of all monitored outgoing messages from D-channel card. A maximum of 5 channels are monitored at a time. Only one channel number can be entered in one command.	
DIS MSGO <dch> DEBG MSG msg1 msg2 msg3		basic-3.0
	Disable the debugging of all monitored outgoing messages from D-channel. This command can be entered more than once. Only 3 message mnemonics can be given in one command.	
DIS MSGO <dch> DEBG SET		basic-3.0
	Disable debug SET on all outgoing messages from D-channel. This set-based filtering is enhanced for UIPE proprietary messages.	
DIS MSGO x FEAT CPNW		basic-21
	Disable outgoing monitoring for the Network CPNW ISDN messages on D Channel x.	
DIS RLB x	Disable remote loop back mode on MSDL DCH x. See "ENL TEST" command for details.	msdl-18
DIS SERV x	Disable service messages on D-channel x. See "ENL SERV" for details. The D-channel must be disabled before disabling service messages.	pra-15

Command	Description	Pack/Rel
DIS TEST x	Disable TEST mode on MSDL DCH x. See "ENL TEST" command for details. When the test mode state is disabled, the DCH link will go back to release state and the DCH background audit will then try to establish the link.	msdl-18
DIS TMDI x (ALL)		
	Disable TMDI card x	basic-24
	For CS 1000S Disable the TMDI card and the various applications on the TMDI. When a DCH is configured on the TMDI, the DCH is released and the DCH application is disabled. The TMDI associated loop is also disabled. Active calls are force disconnected. All channels are disabled.	basic-2.0
DIS TMD I s c u (ALL)		basic-5,0
	Disable TMDI card	
DLIF DCH x	Force download of D channel x (For PRI UIPE application). Note that : 1. D channel specified must use the UIPE application 2. D channel must be disabled 3. D channels configured on the same MSDL card using the same interface must be disabled	uipe-20
DLIF DCH xx FDL		qsig-22
	Force download a PRI interface table. To download the ISDN interface cable: 1. the D channel must be disabled 2. the UIPE application must be active 3. other D channels on the same MSDL card must be disabled	
ENL AUTO x	Enable automatic recovery for DCH x. Automatic recovery is initially enabled.	pra-13
ENL DCH x (FDL)		
	Enable DCH x and attempt to establish the link, and force download to MSDL. A self-test on the DCH runs automatically. If successful, then:	msdl-18

Command	Description	Pack/Rel
	• DCHI status: OPER • DCH status: EST If this is not successful, then: • DCHI status: OPER • DCH status: RLS FDL forces D-channel loadware to the MSDL card. This is optional.	
ENL LLB x	Enable local loop back mode on MSDL DCH x. See "ENL TEST" command for details.	msdl-18
ENL MON ALL	Print messages on the TTY and log them into a file.	pra-5.00
ENL MON LOG	Prepare to log DCH messages into a log file.	pra-5.00
ENL MON TTY	Prepare to print DCH messages on the TTY.	pra-5.00
ENL MSGI x	Enable the monitoring of all incoming messages from D-channel x.	pra-13
ENL MSGI x (options)	Enable the monitoring of all incoming messages from D-channel x. Refer to DIS MSGI x (options) for the list of options.	pra-17
ENL MSGI <dch> DEBG CH <loop><channel>	Enable the debugging of all monitored incoming messages from D-channel card. A maximum of 5 channels are monitored at a time. Only one channel number can be entered in one command.	basic-3.0
ENL MSGI <dch> DEBG MSG msg1 msg2 msg3	Enable the debugging of all monitored incoming messages from D-channel. This command can be entered more than once. In one command, only 3 message mnemonics can be given.	basic-3.0
ENL MSGI <dch> DEBG SET	Enable debug SET on all incoming messages from D-channel This set-based filtering is enhanced for UIPE proprietary messages.	basic-3.0

Command	Description	Pack/Rel
ENL MSGI x FEAT CPNW	Enable incoming monitoring for the Network CPNW ISDN messages on D Channel x.	basic-21
ENL MSGO x (options)	Enable the monitoring of all outgoing messages for D-channel x. Refer to DIS MSGI x (options) for the list of options.	pra-17
ENL MSGO <dch> DEBG CH <loop><channel>	Enable the debugging of all monitored outgoing messages from D-channel card. A maximum of 5 channels are monitored at a time. Only one channel number can be entered in one command.	basic-3.0
ENL MSGO <dch> DEBG MSG msg1 msg2 msg3	Enable the debugging of all monitored outgoing messages from D-channel. This command can be entered more than once. Only 3 message mnemonics can be given in one command.	basic-3.0
ENL MSGO <dch> DEBG SET	Enable debug SET on all outgoing messages from D-channel This set-based filtering is enhanced for UIPE proprietary messages.	basic-3.0
ENL MSGO x FEAT CPNW	Enable outgoing monitoring for the Network CPNW ISDN messages on D Channel x.	basic-21
ENL RLB x	Enable remote loop back mode on MSDL DCH x. See "ENL TEST" command for details.	msdl-18
ENL SERV x	Enable service messages on D-channel x. "Service" and "Service Acknowledge" messages are supported on individual PRA B channels, ISL channels and D-channels. They are used to coordinate channel status between the near and far end. A channel status can be in service, maintenance or out-of-service. The primary and backup D-channel must be disabled before enabling service messages. Make sure both ends support service messages before using this command. By default, SERV is disabled when the interface type is Meridian 1/Meridian SL-1 (LD 17 IFC = SL1).	pra-15

Command	Description	Pack/Rel
	When enabled, service messages are supported on individual PRA B-channels, ISL channels and D-channels. When disabled, service messages are provided automatically on D-channels with Backup D-channel configured. For Meridian 1/Meridian SL-1 to DMS, or Meridian 1/ Meridian SL-1 to AT&T only service messages on individual PRA B- channels and ISL channels are supported. By default, SERV is disabled when the interface type is DMS (LD 17), and enabled when the interface type is AT&T (LD 17 IFC = ESS4/ESS5).	

ENL SSM x y	Enable Supplementary Service Monitor for feature y on D-channel x, where: y = 3 for Network Attendant Service. All other entries are reserved for future use
	Output format is as follows:
	Standard ISDN message monitor output format appended with four fields, where:
	• Field 1 = Customer number
	• Field 2 = Indicator of whether the message is one that was decoded at a "tandem" node
	• Field 3 = Descriptive string about a specified item
	• Field 4 = Numeric information about specified item
	Examples of the four fields follow:
	`--> 002 T-ACCESS TRKINFO`
	`--> 002 T-PRIVATE TRUNK`
	`--> 002 T-TIE TRUNK`
	`--> 002 T-TANDEM COUNT (000001)`
		nas-18

ENL TEST x	Enable TEST mode on MSDL DCH x. The DCH is put into TEST mode to perform the local loop back (LLB) or remote loop back (RLB) test. The DCH link can only be put in test mode if it is in the release or established state. If the link is in establish state, the DCH link is first released, and then put in test mode. The local loop back test first tests the expedited interface, then the ring interface. The test consists of sending a data packet through each interface, which in turn is sent back by Layer 2. This data packet is then validated to ensure that the contents of the data packet are the same that were originally sent. Example:	msdl-18

Command	Description	Pack/Rel
	• ENL TEST x enter TEST mode • ENL LLB x enter local loop back mode • TEST LLB x perform test (results are PASS or FAIL) • DIS LLB x exit local loop back mode The remote loopback test is used to verify the integrity of the physical link. To run the test the far-end must be in the remote loopback mode (ENL RLB x). The DCH running the test (near-end) must be in TEST mode. Example: Far-end: ENL TEST x — enter TEST mode ENL RLB x — enter remote loopback mode DIS RLB x — exit remote loopback mode (after test) DIS TEST x — exit TEST mode and restore link Near-end: ENL TEST x — enter TEST mode TEST RLB x — perform test (results are PASS or FAIL) DIS TEST x — exit TEST mode and restore link If the far end is not an MSDL D-channel, use the RLBK command in LD60 to set up the remote loopback test.	
ENL TMDI x	Enable TMDI card number x	basic-24
ENL TMDI x ALL		basic-24
	Enable all units on TMDI card number x	
	For CS 1000S Enable all applications and units on TMDI card x with the associated loop. When a DCH is configured on the TMDI, a background audit will enable and establish the DCH, once the loop is up. DCH layer 3 should be established within about 30 seconds.	basic-2
ENL TMDI x FDL		basic-24
	Enable TMDI Card number x and force a download. This command only works when the TMDI and loop are disabled. It attempts to force download all required applications to TMDI card and then re-enable the card. When download is completed without error, re-enable the TMDI with ENL TMDI x ALL. Overlay 60, ENLL x can also be used to re-enable the TMDI L1 application and the loop.	

Command	Description	Pack/Rel
	Force download f/w to TMDI is only required if a new PSDL file is created for TMDI f/w.	
ENL TMD l s c u		basic-5.00
	Enable TMDI card	
ENL TMD l s c u (FDL,ALL)		basic-5.00
	Enable TMDI card and force a download	
EST DCH x	Establish multiple frame operation on D-channel x. With the absence of the back-up D channel, issuing the EST DCH x command clears all the B-channels on loop x. If backup D-channel is available, the system switches to the backup D-channel and the B-channels of loop x are not cleared.	pra-13
EST ISPC l ch (N)		ispc-22
	Establish data interface process at the ISPC SLAVE side of an ISPC link at loop (l) and channel (ch), where "N" = the "number of tries" counter. The range for N = 0-(1)-255. When N = 0, the mode is set to AUTOMATIC. This mode requires one TDS slot and one DTR unit. This mode is not recommended for use on Small Systems, CS 1000S systems, or systems loaded with heavy traffic. When N > 0, the process is activated for a period of up to N * 30 minutes. The available range goes from 30 minutes (N = 1) to 128.5 hours or 5 days (N = 255). If no value is entered for N, it defaults to a value of 1. When N = 1, one attempt will be made to establish the data interface process before the ISPC slave D-channel is released.	
FDIS NCAL <DCH#> <conn_id>		qsig gf-22
	Force disconnect the specified call-independent connection as defined by its connection ID number. The connection ID number is a number in the range of 1-9999 that identifies the call independent connection on a given DCH.	
MAP DCH x	Get physical address and switch settings for D-channels. This command outputs the card name and switch settings for D-channels. For example: `MAP DCH`	msdl-18

Command	Description	Pack/Rel
	DCH 15 DCHI 07 DCH 23 MSDL 09 PORT 2	
PCON DCH x	Print configuration parameters on MSDL DCH x. This command outputs the parameters originally downloaded when the D-channel was enabled. The output format is: DCH : x LINK PARAM CONFIRM TIME: hh:mm:ss • MSDL x = 0-15 • PORT x = 0-3 • INTERFACE aaa = SL1, D100, D250, ESS4, S100, etc. • OPER MODE aaa bbb ccc ddd eee , where: - aaa = RS422, RS232 - bbb = DTE, DCE - ccc = USR, NET - ddd = baud rate - eee = clock (EXT or INT CLK) T200 xx (LAPD parameter) T203 xx (LAPD parameter) T200 xx (LAPD parameter) N201 xx (LAPD parameter) K xx (LAPD parameter) N2X4 xx (LAPD parameter if INTERFACE is ITR6)	msdl-18
PLOG DCH x	Print protocol error log-on DCH x. Protocol errors can be the result of PRI transmission problems and re-start procedures, or a protocol mismatch with the far end. The PLOG counters are cleared after the PLOG is printed or the DCH card is enabled. When a protocol counter overflows, the PLOG is printed automatically and the counters are cleared. The counter is also cleared when the D-channel is disabled. Response is: DCH : xx MAINT CONFIRM TIME: hh:mm:ss 01 cc 11 cc 23 cc Where: • x = DCH number • xxxx = system real time (in hexadecimal) • yy = maintenance indication primitive	pra-18

Command	Description	Pack/Rel
	• zz = maintenance indication task ID • 01 02 03....16 = protocol error counters as listed below • cc = protocol error counts Only the non-zero counters are output. Protocol error counters: • 01 = Count of missing PRI handshakes • 02 = Count of peer initiated re-establishment link • 03 = Count of unsuccessful retransmit N200 of SABME • 04 = Count of unsuccessful retransmit N200 of DISC • 05 = Count of N(R) errors • 06 = Count of I fields with length greater than N201 • 07 = Count of undefined frames • 08 = Count of I fields but not allowed • 09 = Count of FRMR frames • 10 = Count of CRC error frames • 11 = Count of REJ frames • 12 = Count of messages with less than 4 octets • 13 = Count of undefined protocol discriminators • 14 = Count of undefined message types • 15 = Count of messages missing mandatory information elements • 16 = Count of messages with undefined information elements • 17 = Count of layer 1 reports of no external clock being received • 18 = Count of aborted frames • 19 = Count of SABME frames received with incorrect C/R bit • 20 = Count of supervisory frames received with F = 1 • 21 = Count of unsolicited DM responses with F = 1 • 22 = Count of unsolicited UA responses with F = 1 • 23 = Count of unsolicited UA responses with F = 0 • 24 = Count of DM responses with F = 0	

Command	Description	Pack/Rel
	• 25 = Number of times that no response was received from the far end after N200 retransmissions of RR or RNR • 26 = Count of frames received with incorrect header length • 27 = Number of times owner receiver busy condition was entered • 28 = Number of times peer receiver busy condition was entered • 29 = Count of messages with call reference length greater than 2 • 30 = Count of optional IEs received with invalid contents • 31 = Count of mandatory IEs received with invalid contents • 32 = Count of messages received with IE's not ordered correctly • 33 = Count of IEs which were repeated in received messages, but are only allowed to appear once per message • 34 = Count of IEs received with length exceeding the specified maximum length for the IE • 35 = Count of layer 3 messages from far-end with invalid call reference flag value of 0. • 36 = Count of layer 3 messages from far-end with invalid call reference flag value of 1. • 37 = Count of layer 3 messages from far-end with invalid global call reference. • 38 = Count of layer 3 messages that are too short. • 39 = Count of layer 3 messages containing an undefined message type. • 40 = Count of layer 3 messages missing mandatory IE(s). • 41 = Count of layer 3 messages containing unsupported IE(s). • 42 = Count of layer 3 messages containing invalid operational IE(s). • 43 = Count of layer 3 messages containing invalid mandatory IE(s).	

Command	Description	Pack/Rel
	• 44 = Count of layer 3 messages with IE(s) out of order. • 45 = Count of layer 3 messages containing repeated IE(s). • 46 = Count of layer 3 messages from far-end with an invalid call reference length. • 47 = Count of layer 3 messages with an invalid call reference flag value of 0. • 48 = Count of layer 3 messages with an invalid call reference flag value of 1. • 49 = Count of layer 3 messages with an invalid global call reference. • 50 = Count of unexpected layer 3 messages received from the far-end. • 51 = Count of unexpected layer 3 messages received from the SL-1. - 52 = Count of unexpected layer 3 timer expirations. - 53 = Count of protocol messages received when D-channel is not in service or waiting for a Service Acknowledge message.	

PMES DCH x	Print incoming layer 3 messages on MSDL DCH x. The following data is kept by the MSDL DCH loadware and output when requested by this command or when one of the counters overflows:
	`DCH : xx`
	`MSG LOG CONFIRM TIME: hh:mm:ss`
	`SETUP: yy`
	`CONNECT: yy`
	`ALERT: yy`
	(Only non-zero counters are reported) (Where yy is the number of times a message was received)
	When a counter overflows, the log is printed automatically and the counters are cleared. The counter is also cleared when the D-channel is disabled.
		msdl-18

PTRF DCH x	Print traffic report on MSDL DCH x. The following traffic information is output:	msdl-18

Command	Description	Pack/Rel
	• PEAK_I_US xx % = peak incoming usage on the DCH link • AVRG_I_US xx % = average incoming usage on the DCH link • PEAK_O_US xx % = peak outgoing usage on the DCH link • AVRG_O_US xx % = average outgoing usage on the DCH link • TIME xx = time in seconds • CONNECTED CALLS xx: = total number of established call-independent connections	
RLS DCH x	Release D-channel x. The link is in a waiting state, ready to come back up at any time. If you release the D-channel with active B-channels, then calls in progress are not affected. However, these calls are disconnected when you re-establish the D-channel. When the automatic recovery feature is active, the B-channels are automatically re-established	pra-13
RLS ISPC l ch	Stop the data interface establishment process. When this command is entered, the mode becomes MANUAL and the number of attempts to be performed = 0.	ispc-22
RST DCH x	Reset D-channel x, inhibit signaling. Forces the link to reset (RST) state, but does not disable PRI or DCH	pra-13
RST MON	Reset or reactivate monitoring on D-channels with enabled monitors.	pra-17
RST TMDI x	Reset TMDI card x	basic-24
RST TMD l s c u		basic-5.00
	Reset TMDI card	
SDCH DCH x	Switch to the standby D-channel x. This is only valid in a backup D-channel configuration. Releases a D-channel and switches over to the other D-channel as long as the other D-channel is in EST STBY, established standby mode. Where x is the standby D-channel number. This command changes the status of the active D-channel	pra-13

Command	Description	Pack/Rel
	to standby, and changes the status of standby D-channel to active. This command is not applicable if the recovery to primary D-channel option (prompt RCVP = YES in LD 17) is used. This command is only applicable to CS 1000to CS 1000Backup D-channel interface (IFC = SL-1 in LD 17).	
SET MSGI x MON (0)-2		pra-17
	Set monitor output format level for all incoming messages on D-channel x. Refer to Setting output format levels earlier in the section.	
SET MSGO x MON (0) -2		pra-17
	Set monitor output format level for all outgoing messages on D-channel x. Refer to Setting output format levels earlier in the section.	
SLFT TMDI x	Invoke self test on TMDI card x	basic-24
SLFT TMD l s c u		basic-5.00
	Invoke self test	
STAT DCH x	Get the present status of D-channel x, where x is the I/O port number (entering x to specify just one link is optional). DCH status may be: • `EST` = DCH link is established • `EST STBY` = DCH link is established and is the standby • `FAIL` = DCH link has failed RLS = DCH link is released • `RST` = DCH link is in reset state • `AEST, ARLS, REST` = these codes indicate intermediate background functions are being performed. Enter the STAT command again to determine final status.	pra-13
STAT DCH (x)		
	Get status of one or all D-channels.	pra-18

Command	Description	Pack/Rel
	If a DCH number is not entered, the status of all D-channels is output. The output format is: `DCH x : aaaa bbbb cccc dddd x` Where: • `x` = DCH number • `aaaa` = application status • `bbbb` = link status • `cccc` = AUTO if autorecovery is enable • `dddd` = BKUP x or PRIM x (associated primary or backup DCH) Application status (`aaaa`): • `APRI` = Awaiting PRI response • `CPRI` = Checking PRI • `DIAG` = application has failed • `DSBL` = application is disabled • `OPER` = link is operational • `RST` = application is in reset state SDCH = Setting D-channel Link status (`bbbb`): • `AEST` = Awaiting establishment • `ARLS` = Awaiting release • `EST ACTV` = DCH link is established and active • `EST STBY` = DCH link is established and is the standby • `FAIL` = DCH link has failed • `REST` = request establishment • `RLS` = DCH link is released • `RST` = DCH link is in reset state • `TST` = Test mode	
STAT DCHI (x)		
	Get the present status of DCHI x (entering x to specify just one card, is optional). DCHI status may be:	pra-13

Command	Description	Pack/Rel
	• DSBL = DCHI hardware is disabled • DIAG = DCHI hardware has failed • OPER = DCHI hardware is operational • RST = DCHI is in reset state • PRI, CPRI, SDCH = these codes indicate intermediate background functions are being performed. Enter the STAT DCHI command again to determine final status.	
STAT ISPC l ch		
	Get status of data interface establishment process at an ISPC SLAVE side of an ISPC link (where l = loop and ch = channel) which is configured to convey D-channel signaling. The status may be: • DISABLED = ISPC link is disabled • AWAITING ESTABLISHMENT = the data interface establishment process is waiting to receive DTMF digits. While waiting, dial tone is provided to the ISPC link at the SLAVE side. • RELEASED = the data interface establishment process is stopped because either an "RLS ISPC" command has been entered or because the maximum number of tries has been reached. • ESTABLISHED = data interfaces at both ends of the ISPC link are established. • AWAITING RELEASE = the ISPC link is being disconnected. Once disconnected, the link will transition to the "RELEASED" state. The mode may be: • MODE MANUAL N = the data interface establishment process is running with up to "N" number of tries • MODE AUTOMATIC = the switch provides dial tone to the ISPC slave D-channel.	ispc-22
STAT MON (x)		
	Display the incoming and outgoing monitoring status of one or all D-channels.	pra-13

Command	Description	Pack/Rel
STAT NCAL <DCH#>	List all current call-independent connections on a given PRI D-channel. The response format is as follows: • NCAL CONN_ID : The connection ID number is a number in the range of 1-9999 that identifies the call independent connection on a given DCH. • CREF : call reference number in HEX identifying independent connection • STATE : current state of all call-independent connections (IDLE, CONN_REQ, CONN_EST) • TIME : year month day hour:minute:second (the time when call independent connection request is made) • APPL : applications using the call-independent connection (eg. NACD, NMS, ...) • ORIG : originator • DEST : destination	qsig gf-22
STAT NCAL <DCH#> <conn_ID>	List information pertaining to a specific call-independent connection as defined by its connection ID number. The response format is as follows: • NCAL CONN_ID : The connection ID number is a number in the range of 1-9999 that identifies the call independent connection on a given DCH. • CREF : call reference number in HEX identifying independent connection • STATE : current state of all call-independent connections (IDLE, CONN_REQ, CONN_EST) • TIME : year month day hour:minute:second (the time when call independent connection request is made) • APPL : applications using the call-independent connection (eg. NACD, NMS, ...) • ORIG : originator • DEST : destination	qsig gf-22

Command	Description	Pack/Rel
STAT SERV (x)		
	Get the enable/disable status of services messages for one or all D-channels. See "ENL SERV" for details.	pra-15
STAT TMDI x	Get TMDI status on card x	basic-24
STAT TMDI x FULL		basic-24
	Get TMDI status and all corresponding units.	
STAT TMD I s c u (FULL)		basic-5.00
	Get TMDI status	
TEST 100 x	Perform interrupt generation test on DCHI x. This is an isolated hardware test. If this test fails, either a faulty DCHI card or a contention problem is indicated. Tests 100, 101, 200, and 201 must be run in sequential order. Established calls will stay up, but new calls cannot be placed. The DCH link must be in the reset (RST) state when these tests are run. Reset (RST) can be established when the status of the D-channel is established (EST) or released (RLS).	pra-13
TEST 101 x	Perform loop back mode test on DCHI x. This is an isolated hardware test. If this test fails, either a faulty DCHI card or a contention problem is indicated.	pra-13
TEST 200 x	Perform interrupt handler test on DCHI x. This is a software test which, when failed, indicates software problems. (Not supported on small system)	pra-13
TEST 201 x	Test interrupt handler-to-link interface path. This is a software test which, when failed, indicates software problems. (Not supported on small system)	pra-13
TEST LLB x	Start local loop back test on MSDL DCH x. See "ENL TEST" command for details.	msdl-18
TEST RLB x	Start remote loop back test on MSDL DCH x. See "ENL TEST" command for details.	msdl-18

Chapter 31: LD 117: Ethernet and Alarm Management

This overlay has a command format that allows the administrator to:

- configure the Alarm Management feature
- identify all system alarms
- configure IP network interface addresses
- perform all IP network related maintenance and diagnostic functions

Both Administration and Maintenance commands appear in this overlay, therefore this overlay is present in both Avaya Communication Server 1000 software reference documents: *Avaya Software Input Output Reference - Administration, NN43001-611* and *Avaya Software Input Output Reference - Maintenance, NN43001-711*.

Command format

LD 117 uses a command line input interface (input parser) that has the following general structure (where "=>" is the command prompt):

=> COMMAND OBJECT [(FIELD1 value) (FIELD2 value)... (FIELDx value)]

LD 117 offers the administrator the following configuration features:

- Context Sensitive Help - Help is offered when "?" is entered. The Help context is determined by the position of the "?" entry in the command line. If you enter "?" in the COMMAND position, Help text appears that presents all applicable command options. If you enter "?" in the OBJECT position, HELP text appears that presents all applicable OBJECT options.
- Abbreviated Inputs - The new input parser recognizes abbreviated inputs for commands, objects and object fields. For example, "N" can be entered for the command "NEW" or "R" can be entered for the object "Route".
- Optional Fields - Object fields with default values can be bypassed by the user on the command line. For example, to configure an object which consists of fields with default values, enter the command, enter the object name, press <return>, and the object is configured with default values. All object fields do not have to be specified. For CS 1000S systems both the optional fields <cab> and <port> refer to the MG 1000S number.

- Selective Change - Instead of searching for a prompt within a lengthy prompt-response sequence, "Selective Change" empowers the administrator to directly access the object field to be changed.
- Service Change Error Message Consistency - The parser simplifies usage of service change error messages. LD 117 displays only SCH0099 and SCH0105.

Alarm Management capability

With the Alarm Management feature, all processor-based system events are processed and logged into a new disk-based System Event List (SEL). Events which are generated as a result of administration activities, such as SCH or ESN error messages, are not logged into the SEL. Events which are generated as a result of maintenance or system activities, like BUG and ERR error messages, are logged into the SEL. Unlike the previous System History File, this new System Event List survives Sysload, Initialization and power failures.

Feature packaging

With the exception of the Alarm Notification subfeature, the Alarm Management feature is optional. It is a major enhancement to the existing Alarm Filtering (ALRM_FILTER) package 243.

The Event Collector

The Event Collector captures and maintains a list of all processor-based system events. The Event Collector also routes critical events to FIL TTY ports and lights the attendant console minor alarm lamp as appropriate. The System Event List (SEL) can be printed or browsed.

The Event Server

The Event Server consists of two components:

1. Event Default Table (EDT): This table associates events with a default severity. By using the CHG EDT command in LD 117, the EDT is overridden so that all events default to a severity of either INFO or MINOR. The EDT is viewed in LD 117. The Default Table is stored in a disk file but is scanned into memory on start-up for rapid run-time access.

Table 18: Sample Event Default Table (EDT)

Error Code	Severity
ERR220	Critical
IOD6	Critical
BUG4001	Minor

Note:
Error codes which do not appear in the EDT is assigned a default severity of MINOR.

2. Event Preference Table (EPT): This table contains site-specific preferences for event severities as well as criteria for severity escalation and alarm suppression. The administrator configures the EPT to:

    a. override the default event severity assigned by the default table

    or

    b. escalate event severity of frequently occurring minor or major alarms.

Table 19: Sample Event Preference Table (EPT)

Error Code	Severity	Escalate Threshold (events/60 sec.) (see Note 2)
ERR??? (see Note 1)	Critical	5
INI???	Default	7
BUG1??	Minor	0
HWI363	Major	3

Note:
The "?" is a wildcard. See the section below for explanation of wildcard entries.

Note:
The window timer length defaults to 60 seconds. However, this value can be changed by the Administrator. Read Global window timer length on page 364 for more information.

Wildcards

The special wildcard character "?" can be entered for the numeric segment of an error code entry in the EPT to represent a range of events. All events in the range indicated by the wildcard entry can then be assigned a particular severity or escalation threshold.

For example, if "ERR????" is entered and assigned a MAJOR severity in the EPT, all events from ERR0000 to ERR9999 are assigned MAJOR severity. If "BUG3?" is entered and assigned

an escalation threshold of 5, the severity of all events from BUG0030 to BUG0039 is escalated to the next higher severity if their occurrence rate exceeds 5 per time window.

The wildcard character format is as follows:

- ERR? = ERR0000 - ERR0009
- ERR?? = ERR0010 - ERR099
- ERR??? = ERR0100 - ERR0999
- ERR???? = ERR1000 - ERR9999

Escalation and suppression thresholds

The escalation threshold specifies a number of events per window timer length that, when exceeded, causes the event severity to be escalated up one level. The window timer length is set to 1 minute by default. Escalation occurs only for minor or major alarms. Escalation threshold values must be less than the universal suppression threshold value.

A suppression threshold suppresses events that flood the system and applies to all events. It is set to 15 events per minute by default.

Global window timer length

Both the escalation and suppression thresholds are measured within a global window timer length. The window timer length is set to 1 minute by default. However, the window timer length can be changed by using the CHG TIMER command in LD 117.

TTY output format of events

TTY event output can be formatted or unformatted. Formatted output is also called fancy format. Output format is configurable in LD 117 using the CHG FMT _OUTPUT command.

Fancy format output

Formatted output appears in the following template:<severity> <report id> <date> <time> <prim_seq_no> <cp_id> <cp_ad> DESCTXT: <descriptive text> OPRDATA: <operator data> EXPDATA: <expert data>

Field	Description
<severity>	"***" (critical); "**" (major); "*" (minor); " " (blank for info)
<report id>	The report ID consists of an event category (e.g. BUG, ERR, etc.) and an event number (1200, 230, etc.). It is padded with blanks at the end to ensure it is 9 characters long (4 characters maximum for category and 5 digits maximum for number). Examples of report IDs are: ACDxxxx, ERRxxx and BUGxx, where x = 0-9.
<date>	DD/MM/YY
<time>	HH:MM:SS
<prim_seq_no>	Primary sequence number of the event (length of 5 digits)
<cp_id>	The Component ID is a 15 character string which indicates the ID of the subsystem generating the alarm
<cp_ad>	The Component address is a 15 character string which indicates the address of the subsystem generating the event
<descriptive text>	This is an optional string which describes an event
<operator data>	This is an optional field which holds a 160 character string containing extra text or data to assist the operator in clearing a fault. This field contains any data output with a filtered SL-1 alarm (e.g. loop number, TN, etc.)
<expert data>	This is an optional variable length character string which contains extra text or data for a system expert or designer.

The following are samples of fancy format output:

```
*** BUG015 15/12/95 12:05:45  00345
EXPDATA: 04BEF0FC 05500FBA  05500EE2  05500EC6 05500EAA
BUG015 + 05500E72 + 05500E56 + 0550D96 + 055053A + 04D84E02 + 04D83CFC
BUG015 + 04D835CA 04D81BAE 04D7EABE 04F7EABE 04F7EDF2 04F7EFC 04F7E1B0
*      ERR00220 15/12/92 12:05:27 00346
OPRDATA: 51
VAS0010 15/12/92 12:06:11 00347 VMBA     VAS 5
```

Unformatted Output

Unformatted data consists of only the report ID and perhaps additional text. The following is a sample of unformatted output:

```
BUG015
BUG015 + 04BEF0FC 05500FBA 05500EE2 05500EAA 0550E8E
BUG015 + 05500E72 05500E56 05500D96 0550053A 04D84E02
BUG015 + 04D835CA 04D81BAE 04D7EABE 04F7EDF2 04F7E2FC 04&E1B0
BUG015 + 04F7E148
ERR00220 51
VAS0010
```

Ethernet and Point-to-Point Protocol

LD 117 is used to configure and manage an IP network interface. The large systems are hardware-equipped with an Ethernet controller on the I/O processor (IOP) card. Each IOP card is equipped with a Local Area Network Controller for Ethernet (LANCE) which is preconfigured with an unique Ethernet address.

The Small Systems and CS 1000S systems can be hardware-equipped with Ethernet daughterboards on the System Controller card. They support both Ethernet and Point-to-Point Protocol.

For large systems, the unique 48-bit long physical address (Ethernet address) is a assigned to the Ethernet controller on the IOP. On a single CPU M1 system, there is only one IOP which contains one Ethernet interface and an IP address which must be configured. Single CPU systems use only a Primary IP address.

On a redundant or dual CPU M1 system, two IP addresses must be specified: Primary and Secondary. A dual CPU M1 system operating normally uses the Primary IP address. A dual CPU M1 system operating in split mode (the mode used only when upgrading software or hardware) uses the Secondary IP address.

Remote access to the switches is made possible with Point-to-Point Protocol (PPP). LD 117 is used to configure IP addresses for Point-to-Point Protocol.

The large system Ethernet interface is provided by the IOP card with AUI cable on the back panel on Options 51C, 61C, 81 and 81C. The Small System provides an Ethernet interface through an ethernet connection on the main cabinet. The CS 1000S system provides an Ethernet interface through an ethernet connection on the Call Server. The Point-to-Point Protocol (PPP) is established via asynchronous connection to any system SDI port. The IP addresses for Ethernet and PPP interface are configured in Overlay 117, and defaults are available for all new installations and upgrades.

How to Configure Ethernet and Point-to-Point Protocol

The following tables explain how to configure IP addresses for Ethernet and Point-to-Point Protocol. These two tables are followed by examples.

Configure ELAN IP address for the Ethernet Interface (10BaseT)	
Step	**Action**
1	Load Overlay 117
2	Create host entries
3	Assign host to primary and/or secondary IP address(es)
4	Set up Ethernet subnet mask

Configure ELAN IP address for the Ethernet Interface (10BaseT)	
Step	**Action**
5	Set up routing entry

Configure ELAN IP address for the Point-to-Point Protocol Interface (10BaseT)	
Step	**Action**
1	Load Overlay 117
2	Create host entries
3	Assign host to primary and/or secondary IP address(es)

Example 1 Configure ELAN IP address for the Ethernet Interface (10BaseT)

Given: Primary IP address: 47.1.1.10 ; Secondary IP address: 47.1.1.11; Subnet mask: 255.255.255.0; Default Gateway IP: 47.1.1.1

Step	Action
1	Load Overlay 117
2	Create host entries. Enter one of the following commands: NEW HOST PRIMARY_IP 47.1.1.10 NEW HOST GATEWAY_IP 47.1.1.1 (if connected to customer LAN) NEW HOST GATEWAY_IP 47.1.1.1 (if connected to customer LAN)
3	Assign host to primary and/or secondary IP address(es). Enter one of the following commands: CHG ELNK ACTIVE PRIMARY_IP CHG ELNK INACTIVE SECONDARY_IP (for Dual CPU only) Verify your IP address for Ethernet by entering the PRT ENLK command. **Note:** To reuse the active host entry and/or associated IP address, the existing entry must be removed. Prior to removing the existing enty, you must first create a temporary host entry and make it active. Out the original host entry, then proceed to Step 2.
4	Set up Ethernet subnet mask. Enter the command: CHG MASK 255.255.255.0 Verify subnet mask setting by entering the command: PRT MASK
5	Set up routing entry. Enter the command: NEW ROUTE 0.0.0.0 47.1.1.1 (if connected to customer LAN) Where: 0.0.0.0 = destination network IP and 47.1.1.1 = default gateway IP **Note:** When more than one gateway exists, replace 0.0.0.0 with the destination network address for each entry of the routing table. Verify default routing by entering the command: PRT ROUTE

Example 1 Configure ELAN IP address for the Ethernet Interface (10BaseT)

Note:
For a single CPU machine, the secondary IP is not used.

Note:
The secondary IP is accessible only when a system is in split mode.

Note:
The subnet mask must be the same value used for the system Ethernet network.

Note:
The system private Ethernet (ELAN subnet) is used for system access and control. Use an internet gateway to isolate the system private Ethernet from the Customer Enterprise Network.

Note:
Routing information is required if an internet gateway or router connects a system private network (ELAN subnet) to the Customer Enterprise Network. New routes use network IPV4 classification to determine the whether the route is network or host based.

Note:
INI is required for the activation of subnet Mask.

Example 2 Configure ELAN IP address for the Point-to-Point Protocol Interface (10BaseT)

Given: Local IP address: 172.1.1.1; Remote IP address 100.1.1.1

Step	Action
1	Load Overlay 117
2	Create host entries. Enter one of the following commands: NEW HOST LOCAL_PPP 172.1.1.1 NEW HOST REMOTE_PPP 100.1.1.1 (this entry is optional)
3	Assign host to primary and/or secondary IP address(es). Enter one of the following commands: CHG PPP LOCAL LOCAL_PPP 0 (always use interface #0) CHG PPP REMOTE REMOTE_PPP 0 (this entry is optional) Verify your IP address(es) for PPP by entering the PRT PPP command.

Command descriptions

Command	Definition	Description
****	Abort	Abort overlay or Printing if it is printing an Inventory file
BROWSE	Browse	Browse an existing System Event List
CHG	Change	Change/modify object configuration
DIS	Disable	Disable Point-to-Point Protocol
ENL	Enable	Enable Point-to-Point Protocol
INV GENERATE	Enable	Enable inventory
INV MIDNIGHT	Enable	Set Midnight routine for inventory
INV PRT	Print	Print out the status of the Inventory feature
NEW	New	Add and configure new object
OUT	Out	Delete existing object
PRT	Print	Print configuration of existing object
RST	Reset	Reset Object
SET	Set	Set ELNK subnet mask to configured value
STAT	Status	Display object statistics
STIP	Status	Display resource locator module information
TEST	Test	Test Object
UPDATE	Update	Update INET database

Object descriptions

Object	Description
DBS	Database
DNIP	IP address of IP Phone
EDT	Event Default Table: Table of default event entries and associated severities

Object	Description
ELNK	Ethernet interface
ELNK ACTIVE	Active Ethernet Link: Change the Primary IP address and host name
ELNK INACTIVE	Inactive Ethernet Link: Change the Secondary IP address and host name
EPT	Event Preference Table: Table of customer's event entries with associated severities
FMT_OUTPUT	Formatted Output: Determine if system events uses formatted (also called fancy) or unformatted output.
HOST	Host name
IPDN	IP address of configured DN
IPR	IP connectivity configuration associated with specified port
IPM	IP connectivity configuration associated with main cabinet
LDAPSYNC	LDAP server synchronization
MASK	Subnet mask
NDAPP	Name Directory application
OPEN_ALARM	Open Simple Network Management Protocol (SNMP) traps setting
PPP	Point-to-Point Protocol interface
PPP LOCAL	Local Point-to-Point Protocol interface address
PPP REMOTE	Remote Point-to-Point Protocol interface address
PTM	Point-to-Point Protocol idle Timer
ROUTE	Configure new routing entry
SELSIZE	System Event List Size: Number of events in System Event Log
SEL	System Event List
SUPPRESS	Number of times the same event is processed before it is suppressed.
SUPPRESS_ALARM	Severity level that triggers sending of alarms.
TIMER	Global window timer length

How to configure IP Connectivity with CS 1000S

The following tables explain IP Connectivity set-up using Bootp and Manual Configuration. The tables are followed by examples.

Important:
CS 1000S does not support IP addresses of all zeros (0) or all ones (1).

Point-to-Point configuration - Call Server, Bootp is used

To configure Mac addresses for the MG 1000S 100BaseT daughterboard in a Point-to-Point configuration, use the following steps. Full IP connectivity configuration for the system is done on the Call Server side in OVL117. Bootp protocol is used to automatically configure IP parameter on the MG 1000S.

Configure MAC address for the 100BaseT daughterboard.	
Step	**Action**
1	Load Overlay 117.
2	Configure MAC address.
3	Reboot Call Server.

Example 1 Configure MAC address for the 100BaseT daughterboard.	
Given:	MAC address of the 100BaseT daughterboard on the MG 1000S: 00:90:cf:03:71:15 The MG 1000S is connected to the port number 1 of the Call Server.
Step	Action
1	Load Overlay 117.
2	Configure the MAC address. Enter the following commands: CHG IPR 1 00:90:cf:03:71:15 Verify the MAC address by entering the PRT IPR command.
3	Reboot the Call Server.

Recommended BootP configuration for Layer 2 LAN configuration - Call Server only

The following tables explain how to configure MAC and IP addresses for the 100BaseT daughterboard in a Layer 2 LAN configuration. Full IP connectivity configuration for the system occurs on the Call Server side in OVL117. The MG 1000S does not need to be configured. Bootp protocol is used to automatically configure IP parameter on the MG 1000S. BootP is the recommended Layer 2 configuration procedure.

Configure MAC and IP addresses for the Call Server and MG 1000S TLAN 100BaseT ports.	
Step	**Action**
1	Load Overlay 117.
2	Configure the MAC and IP address of the MG 1000S 100BaseT.
3	Configure the IP address of the Call Server 100BaseT.
4	Reboot the Call Server.

Example 2 Configure MAC and IP addresses for the Call Server and MG 1000S TLAN 100BaseT ports.	
Given:	MAC address of the 100BaseT daughter board on the MG 1000S: 00:90:cf:03:71:15; IP address of the MG 1000S 100BaseT: 47.147.75.101; Subnet Mask of the MG 1000S 100BaseT: 255.255.255.0; IP address of the Call Server 100BaseT: 47.147.75.100; Subnet Mask of the Call Server 100Base: 255.255.255.0; The MG 1000S is connected to the slot number 1 of the Call Server.
Step	Action
1	Load Overlay 117
2	Configure the MAC and IP address of the MG 1000S 100BaseT. Enter the following command: CHG IPR 1 00:90:cf:03:71:15 47.147.75.101 255.255.255.0 YES Verify by entering the command: PRT IPR 1
3	Configure the IP address of the Call Server 100BaseT. Enter the following command: CHG IPM 1 47.147.75.100 255.255.255.0 Verify by entering command: PRT IPM 1
4	Reboot the Call Server.

Manual Layer 2 configuration - Call Server and MG 1000S

When using manual configuration the following steps are required for both the Call Server and MG 1000S.

IP connectivity Layer 2 configuration for the Call Server side occurs in OVL117. These steps are followed to configure MAC and IP addresses for the 100BaseT daughterboard in a Layer 2 configuration on the Call Server side:

Configure MAC and IP addresses for the Call Server TLAN 100BaseT ports and subnet mask.	
Step	**Action**
1	Load Overlay 117.
2	Configure the MAC and IP address of the MG 1000S 100BaseT.
3	Configure the IP address on the Call Server 100BaseT.
4	Reboot the Call Server.

Example 3 Configure MAC and IP addresses for the Call Server TLAN 100BaseT ports and subnet mask.	
Given:	IP address of the Call Server 100BaseT: 47.147.75.100; Subnet Mask of the Call Server 100BaseT: 255.255.255.0; The MG 1000S 1 is connected to the port number 1 of the 100BaseT daughterboard on the Call Server.
Step	Action
1	Load Overlay 117.
2	Configure the MAC and IP address of the MG 1000S 100BaseT. Enter the following command: CHG IPR 1 00:90:cf:03:71:15 47.147.75.101 255.255.255.0 YES Verify by entering the command: PRT IPR 1
3	Configure the IP address of the Call Server 100BaseT. Enter the following command: CHG IPM 1 47.147.75.100 255.255.255.0 Verify by entering the command: PRT IPM 1
4	Reboot the Call Server.

The Layer 2 IP connectivity configuration for the MG 1000S side occurs during system installation when Manual configuration has been chosen. These steps are followed to configure IP address for the 100BaseT daughter board in a Layer 2 configuration on the MG 1000S side: TTY needs to be connected to the MG 1000S.

Configure MAC and IP address for MG 1000S TLAN 100BaseT port.	
Step	**Action**
1	Choose Manual configuration option from the installation menu.
2	Configure the IP address of the MG 1000S 100BaseT.
3	Configure the MG 1000S NetMask.
4	Configure the IP address of the Call Server.

Example 4 Configure MAC and IP address for MG 1000S TLAN 100BaseT port.	
Given:	IP address of the MG 1000S 100BaseT: 47.147.75.101;

Example 4 Configure MAC and IP address for MG 1000S TLAN 100BaseT port.	
	Subnet Mask of the MG 1000S 100BaseT: 255.255.255.0; IP address of the Call Server 100BaseT: 47.147.75.100; The MG 1000S is connected to slot number 1 of the Call Server.
Step	Action
1	IP parameters for this module are obtained by: 1. Automatically using BootP 2. Using Manual configuration
2	Enter the MG 1000S IP address: 47.147.75.101 Enter the MG 1000S NetMask: 255.255.255.0 Enter the Call Server IP address: 47.147.75.100 **Note:** If the MG 1000S IP address is on a subnet different than the Call Server IP address then the default MG 1000S Address (0.0.0.0) is required.

Manual Layer 3 configuration - Call Server and MG 1000S

The IP connectivity Layer 3 for the Call Server is configured in OVL117.

Note:
For Layer 3, manual configuration is mandatory.

These steps are followed to configure MAC and IP addresses for the 100BaseT daughterboard in a Layer 3 configuration on the Call Server side:

Configure MAC and IP address and routing entry for the Call Server TLAN 100BaseT ports.	
Step	**Action**
1	Load Overlay 117.
2	Configure the MAC and IP address of the MG 1000S 100BaseT.
3	Configure the IP address of the Call Server 100BaseT.
4	Configure routing entry between the Call Server and MG 1000S.
5	Reboot the Call Server.

Example 5 Configure MAC and IP address and routing entry for the Call Server TLAN 100BaseT ports.	
Given:	IP address of the Call Server 100BaseT port 1: 47.147.10.100; Subnet Mask of the Call Server 100BaseT: 255.255.255.0; Gateway address on

Example 5 Configure MAC and IP address and routing entry for the Call Server TLAN 100BaseT ports.	
	Call Server: 47.147.10.1; IP address of the MG 1000S 1: 47.147.20.101 The MG 1000S 1 is connected to the port number 1 of the 100BaseT daughterboard on the Call Server.
Step	Action
1	Load Overlay 117.
2	Configure the MAC and IP address of the MG 1000S 100BaseT. Enter the following command: CHG IPR 1 00:90:cf:03:71:15 47.147.20.101 255.255.255.0 YES Verify by entering the command: PRT IPR 1
3	Configure IP address of the Call Server 100BaseT. Enter the following command: CHG IPM 1 47.147.10.100 255.255.255.0 Verify by entering command: PRT IPM 1
4	Configure new route to reach IPR: NEW ROUTE 47.147.20.0 47.147.10.1 0 1
5	Configure new route to reach IPM Local subnet: NEW ROUTE 47.147.10.0 47.147.20.100 0 1
6	Reboot Call Server.

The Layer 3 IP connectivity configuration for the MG 1000S side is configured during system installation when Manual configuration has been chosen. These steps are followed to configure IP address for the 100BaseT daughterboard in a Layer 3 configuration on the MG 1000S side:

Configure MAC and IP address and router entry for MG 1000S TLAN (100BaseT) port.	
Step	**Action**
1	Choose the Manual configuration option from the installation menu.
2	Configure the IP address of the MG 1000S 100BaseT.
3	Configure the IP MG 1000S NetMask.
4	Configure the IP address on the Call Server.
5	Configure the MG 1000S Routing address.

Example 6 Configure MAC and IP address and router entry for MG 1000S TLAN (100BaseT) port.	
Given:	IP address of the MG 1000S 100BaseT: 47.147.20.101; Subnet Mask of the MG 1000S 100BaseT: 255.255.255.0; Gateway address for MG 1000S: 47.147.20.1; IP address of the Call Server 100BaseT: 47.147.10.100; The MG 1000S is connected to slot number 1 of the Call Server.

Example 6 Configure MAC and IP address and router entry for MG 1000S TLAN (100BaseT) port.	
Step	Action
1	IP parameters for this module are obtained by: 1. Automatically using BootP 2. Using Manual configuration Enter your selection: 2
2	Enter the MG 1000S IP address: 47.147.20.101 Enter the MG 1000S NetMask: 255.255.255.0 Enter the Call Server IP address: 47.147.10.100 Enter the MG 1000S Router/Gateway address: 47.147.20.1

Auto-Negotiate on 100BaseT ports

The Auto-Negotiation feature must be enabled on each Main Cabinet/Call Server and Expansion Cabinet/MG 1000S ethernet port to allow bandwidth negotiation of 100 Mbps full duplex.

Note:
These commands are executed on the Main Cabinet/Call Server side.

The commands for enabling auto-negotiation are:

- Main Cabinet/Call Server ports CHG AUTONEG IPM <port> <a...a>
- Expansion Cabinet/MG 1000S port CHG AUTONEG IPR <port> <a...a>

To enable Auto-Negotiation with a Expansion Cabinet/MG 1000S configured on port one, enter the following commands:

CHG AUTONEG IPM 1 ON

CHG AUTONEG IPR 1 ON

Important:
When auto-negotiation is enabled, if a link is already up, a LINK DOWN message is reported on the TTY. This is normal because the data ports must perform the bandwidth negotiation protocol to obtain its required 100Mbps full duplex. This process takes 5 to 7 seconds. Once the process is complete, a LINK UP message is reported and the system is ready for normal operations.

To get the status of the auto-negotiation process, after process completion, enter the following commands:

STAT AUTONEG IPM

STAT AUTONEG IPR

The following is a sample print out for the Main Cabinet/Call Server:

```
AUTO-NEGOTIATE LINK PARTNER STATUS - MAIN/CALL
SERVER PORTS
-------------------------------------------------
PORT Bandwidth Duplex Mode AutoNegotiate
=================================================
IPM 1 UNKNOWN UNKNOWN ON
IPM 2 UNKNOWN UNKNOWN
IPM 3 100 Mbps  full duplex  ON
IPM 4 UNKNOWN UNKNOWN
```

If the auto-negotiation process is successful, it returns " 100 Mbps full duplex". Otherwise UNKNOWN is reported, indicating a failure in negotiating the 100 Mbps full duplex bandwidth.

The following is a sample print out for the MG 1000S:

```
AUTO-NEGOTIATE LINK PARTNER STATUS - EXPANSION/MEDIA GATEWAY PORTS
-------------------------------------------------
PORT Bandwidth Duplex Mode AutoNegotiate
=================================================
IPR 1 UNKNOWN UNKNOWN ON
IPR 2 UNKNOWN UNKNOWN
IPR 3 100 Mbps  full duplex  ON
IPR 4 UNKNOWN UNKNOWN
```

If the auto-negotiation process is successful, it returns " 100 Mbps full duplex". Otherwise UNKNOWN is reported, indicating a failure in negotiating the 100 Mbps full duplex bandwidth.

IP command descriptions

Command	Description
CHG AUTONEG IPM	Change Auto-Negotiation for Main Cabinet ports.
CHG AUTONEG IPR	Change Auto-Negotiation for Expansion Cabinet port.
CHG AUTOSB <cab> <a...a>	Change the automatic switch back option of a given Expansion Cabinet.
CHG CACVT <Zone> <1-(48)-255>	Configure the zone-to-zone record validity time interval. Where:

Command	Description
	• Zone = 0–255 • Zone = 0–8000 • 1-(48)-255 = interval in hours
`CHG CD <Zone> <1-(50)-100>`	Change the Cd coefficient in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone. Where: • Zone = 0–255 • Zone = 0–8000 • 1-(50)-100 = Cd coefficient
`CHG CPL <Zone> <1-(50)-100>`	Change the Cpl coefficient in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone. Where: • Zone = 0–255 • Zone = 0–8000 • 1-(50)-100 = Cpl coefficient
`CHG ES1 <Echo Server IP Address> <Echo Server Port>`	Change Echo Server 1's IP address and port number. Where: • Echo Server 1 IP Address = (0.0.0.0) • Echo Server 1 Port number = (10000) **Note:** Echo Server 1 IP address uses the TLAN IP address of the LTPS card.
`CHG ES2 <Echo Server IP Address> <Echo Server Port>`	Change the Echo Server 2 IP address and port number. Where: • Echo Server 2 IP Address = (0.0.0.0) • Echo Server 2 Port number = (10000) **Note:** Echo Server 2 IP address uses the node IP address on the node's master card.

Command	Description
CHG IPM <port> <ip> [mask]	Changes the IP connectivity configuration associated with the Main Cabinet end of the specified port.
CHG IPR <port> <mac> [ip] [mask] [a...a]	Change the IP connectivity configuration data associated with the Expansion Cabinet end of the specified port. Where: a...a = zeroBandwidth = (NO) YES Default value for zeroBandwidth means that in a 'no traffic condition' bandwidth is not brought down to zero. Use NO in a PTP configuration, when data units are configured on the Expansion Cabinet to avoid potential packet loss. Use YES in a Layer 2 or Layer 3 configuration to bring the bandwidth down to zero in a no traffic condition.
CHG NKT	Change NAT Mapping Keep Alive time-out setting of port mapping for devices behind a NAT router. Where time out setting = 0-(30)-60 seconds.
CHG NUMZONE <numbering zone> <site_prefix> <country_code> <npa> <ac1> <ac2> <natc> <intc> <dac> <ttbl>	Change the parameters of a ZBD numbering zone. Package 420 (Zone Based Dialing) must be equipped.
CHG NZDES <numbering zone> <description>	Change the description of a ZBD numbering zone. Package 420 (Zone Based Dialing) must be equipped.
CHG PDV <port> <delay>	Set Packet Delay Variation (PDV) buffer size and delay.
CHG PPP LOCAL <hostname> [cab]	Set CS 1000S local Point-to-point Protocol interface IP address.
CHG PPP REMOTE <hostname> [cab]	Set CS 1000S remote Point-to-point Protocol interface IP address.
CHG PTM <xx> [cab]	Change Point-to-Point Protocol Timer.
CHG SWOTO <cab> <x...x>	Change the switch over time out timer of a given MG 1000S.
CHG SURV <cab> <a...a>	Change Survivable Capability of a given MG 1000S.

Command	Description
CHG ZACB <Zone> <AC1-AC2> <AC1-AC2>	Define the access codes used to modify local calls in the branch office zone.
CHG ZBRN <Zone> <a...a>	Define a zone as a branch office zone.
CHG ZDES <Zone> <ZoneDescription>	Assign the Zone a descriptive name (ZoneDescription).
CHG ZDID <numbering zone> <matching string> <replacement string> [<description>]	Change a ZBD numbering zone-based call translation table entry. Package 420 (Zone Based Dialing) must be equipped.
CHG ZDP <Zone> <DialingCode1> <DialingCode2> <DialingCode3>	Define the dialing plan for the branch office zone.
CHG ZDST <Zone> a...a <StartMonth> <StartWeek> <StartDay> <StartHour> <EndMonth> <EndWeek> <EndDay> <EndHour>	Specify whether the branch office zone observes daylight savings time.
CHG ZESA <Zone> <ESARLI> <ESAPrefix> <ESALocator>	Defines the emergency services access (ESA) parameters for the branch office zone. These parameters are used only if the ESA package is enabled.
CHG ZFDP <numbering zone> <matching string> <type> [<replacement string>] [LEN <max length>] ["<description>"]	Change a ZBD numbering zone-based flexible dialing plan table entry. Package 420 (Zone Based Dialing) must be equipped.
CHG ZONE <ZoneNumber> <intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <a...a>	Change the parameters of an existing Zone. Where: • <ZoneNumber> = 0–255 • <ZoneNumber> = 0–8000 • <intraZoneBandwidth> = Intrazone available bandwidth (0 to 0.1MBps) • <intraZoneStrategy> = BQ or BB, Intrazone preferred strategy (BQ for Best Quality or BB for best Bandwidth) • <interZoneBandwidth> = Interzone available bandwidth (0 to 0.1MBps)

Command	Description
	• <interZoneStrategy> = BQ or BB, Interzone perferred strategy ((BQ for Best Quality or BB for best Bandwidth) • <a...a> = type of zone (Shared or Private) - **Shared**: The ethersets configured in Shared zones use DSP resources configured in Shared zones. If all of the Shared zones' gateway channels are used, the caller receives an overflow tone and the call is blocked. The order of channel selection for the gateway channels is: i. channel from same zone as etherset is configured ii. any available channel from the shared zones' channels - **Private**: DSP channels configured in a Private zone are used only by ethersets which have also been configured for that Private zone. If more DSP resources are required by these ethersets than what are available in the zone, DSPs from other zones are used. However, ethersets configured in shared zones cannot use the private zones' channels. The order of selection for the gateway channels is: i. channel from same private zone as etherset is configured ii. any available channel from the pool of shared zones' channels **Note:** Current default zone type = Shared. **Note:** All parameters must be re-entered when changing a zone.
`CHG ZPARM <numbering zone> <parameter name> <value>`	Package 420 (Zone Based Dialing) must be equipped.
`CHG ZTDF <Zone> <TimeDifferenceFromHeadOffice>`	Specify the time difference between the Main Office and the branch office when both are not in Daylight Saving Time.

Command	Description
DIS ZBR <Zone> [ALL] [LOC] [ESA] [TIM]	Disable features of the branch office zone.
DWL DBS [cab]	Download 100BaseT database to the specified Expansion Cabinet.
ENL ZBR <Zone> [ALL] [LOC] [ESA] [TIM]	Enable features for the branch office zone.
GEN ZONEFILE <fileName>	Generate a CSV file that contains information for all configured zones on the Call Server. **Caution:** In Release 7.0 and later, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you must use bandwidth zone numbers in the range 0–255; call processing issues occur if you use bandwidth zone numbers greater than 255.
IMPORT ZONEFILE <fileName>	Read a CSV file and create new zones listed in the file, or apply updates contained in the CSV file for zones that already exist. **Caution:** Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you must use bandwidth zone numbers in the range 0–255; call processing issues occur if you use bandwidth zone numbers greater than 255.
NEW HOST <hostname> <IPaddress> [cab]	Configure a new host entry (add host name and IP address to network host table). To reuse the active host entry and/or associated IP address, the existing host entry must be removed. Prior to removing the existing host entry, you must first create a temporary host entry and make it active. OUT the original host entry and re-create your intended host entry. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network

Command	Description
	configuration and management are controlled from the Linux Base layer.
NEW NUMZONE <numbering zone> [<site_prefix> <country_code> <npa> <ac1> <ac2> <natc> <intc> <dac> <ttbl>]	Configure a new ZBD numbering zone. Package 420 (Zone Based Dialing) must be equipped.
NEW RANGE_OF_ZONES <zoneStartNumber> <zoneAmount> <intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <zoneIntent> <zoneResourceType>	Create new bandwidth zones. This command creates a range of new bandwidth zones starting from **<zoneStartNumber>**. The number of existing bandwidth zones must be less than 8001. If the number of existing bandwidth zones is greater than or equal to 8001, no bandwidth zones are created. **Caution:** Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you must use bandwidth zone numbers in the range 0–255; call processing issues occur if you use bandwidth zone numbers greater than 255.
NEW ROUTE <destination IP> <gateway> [cab] [port]	Configure a new routing entry (add new route to the network routing table). **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.
NEW ZFDP <numbering zone> <matching string> [<replacement string>] [LEN <max length>] [<description>]	Configure a new ZBD numbering zone-based Flexible Dialing Plan. Package 420 (Zone Based Dialing) must be equipped.
NEW ZONE <x...x> p1 p2 p3 p4 <shared/private>	Create a new zone with parameters. **Caution:** Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you must use bandwidth zone numbers in the range 0–255; call processing issues occur if you

Command	Description
	use bandwidth zone numbers greater than 255.
OUT NUMZONE <numbering zone)	Remove a ZBD numbering zone. Package 420 (Zone Based Dialing) must be equipped.
OUT RANGE_OF_ZONES <zoneStartNumber> <zoneAmount>	Remove a range of existing bandwidth zones. This command deletes a range of existing bandwidth zones, starting from <zoneStartNumber>. If there are no bandwidth zones with a zone number greater than <zoneStartNumber>, then no bandwidth zones are deleted.
OUT ZDID <numbering zone> <matching string>	Delete a ZBD numbering zone-based call translation. Package 420 (Zone Based Dialing) must be equipped.
OUT ZFDP <numbering zone> <matching string>	Delete a ZBD numbering zone-based flexible dialing plan. Package 420 (Zone Based Dialing) must be equipped.
PRT AQOS <attribute> <zone / ALL>	Prints QoS records for specified attribute and zone (or for all zones with ALL).
PRT CAB [cab]	Print parameters and survivable capability of the specified Expansion Cabinet.
PRT DNIP <DN> [<CustomerNo>]	Print a list of IP addresses for each IP Phone registered with the specified DN. **Note:** A partial DN can be entered.
PRT ES1	Print Echo Server 1's IP address and port number.
PRT ES2	Print the Echo Server 2 IP address and port number.
PRT ESS	Print both Echo Servers IP address and port number.
PRT INTERZONE	Print interzone statistics for the range between the near and far zones.
PRT INTRAZONE	Print intrazone statistics for all zones or for the specified zone.
PRT IPDN <IPAddress>	Print a list of DNs configured for the specified IP address(es).

Command	Description
	Note: Partial IP addresses can be entered with only the leading digits of the IP address (for example, 142.10), or as the IP address with zeroes at the end (for example, 142.10.0.0)
PRT IPM <port>	Print the IP connectivity configuration data associated with the Main Cabinet end of the specified port.
PRT IPR <port>	Print the IP connectivity configuration data associated with the Expansion Cabinet end of the specified port.
PRT NKT	Print NAT Mapping Keep Alive time-out setting of port mapping for devices behind a NAT router.
PRT NUMZONE <numbering zone)	Print a table of information for a ZBD numbering zone. Package 420 (Zone Based Dialing) must be equipped.
PRT NZDES [<numbering zone>]	Print the description for a specified ZBD numbering zone. Package 420 (Zone Based Dialing) must be equipped.
PRT PDV <port>	Print the current size of the PDV buffer and the number of PDV underflows
PRT PPP [cab]	Print Point-to-point Protocol interface address(es)
PRT PTM [cab]	Print Point-to-Point Protocol idle timer settings
PRT QOS <cab>	Print level of service based on system configured thresholds for selected Expansion Cabinet.
PRT SURV [cab]	Prints the Expansion Cabinet Survivable capability for all, or specified Expansion Cabinets.
PRT ZACB [<Zone>]	Print a table of branch office zone dialing plan entries.
PRT ZBW [<Zone>]	Print a table of zone bandwidth utilization.
PRT ZDES [<DESMatchString>]	Print a table of the zone description entries.

Command	Description
PRT ZDID [<numbering zone>] [<matching string>]	Print a table of ZBD numbering zone-based call translations. Package 420 (Zone Based Dialing) must be equipped.
PRT ZDP [<Zone>]	Print a table of branch office zone dialing plan entries.
PRT ZDST [<Zone>]	Print a table of branch office zone time adjustment properties entries.
PRT ZESA [<Zone>]	Print a table of branch office zone emergency services access (ESA) entries.
PRT ZFDP [<numbering zone>] [<matching string>]	Print a table of ZBD numbering zone-based flexible dialing plans. Package 420 (Zone Based Dialing) must be equipped.
PRT ZONE ALL	Print zone information for all zones.
PRT ZONE x...x	Print zone information for a specific zone.
PRT ZPAGE [<zone number> <zonesPerPage>]	Print zone information for <zonesPerPage> zones starting at <zoneNumber> zone.
PRT ZPARM [<numbering zone>]	Print the parameters of a ZBD numbering zone. Package 420 (Zone Based Dialing) must be equipped.
PRT ZQOS <zone> <attribute / ALL>	Prints QoS records for specified attribute and zone (or for all attributes with ALL).
PRT ZTDF [<Zone>]	Print a table of branch office zone time adjustment properties entries.
PRT ZTP [<Zone>]	Print a table of branch office zone time adjustment properties entries.
PING ipAddress	Ping far end IP address. • When IP (voice) link is UP: PING to/from 100BaseT is ONLY enabled among the Call Server and the Expansion Cabinets. They do not respond to PING from/to any other device in the data network. • When IP (voice) link is DOWN: PING command is enabled to/from entire data network. **Note:** This command is blocked for co-resident Call Server applications (Call Server and

Command	Description
	Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.
STAT LINK APP <applicationType>	Display the link information status of the server for the specified application. Where <applicationType> is: • LTPS (Line TPS) • VGW (Voice Gateway) • H323 (H.323 Virtual Trunk) • GK (GateKeeper)
STAT LINK IP <IP address>	Display the link information status of the server for the specified IP address, or IP addresses of the specified sub-net. Where <IP address> = the ELAN IP address of the Signaling Server or Voice Gateway Media Card. **Note:** The IP address can be in full or partial IP address format (e.g., "10.11.12.13" or "10.11").
STAT LINK NAME <hostName>	Display the link information status of the servers based on the supplied host name. Where <hostName> = MAINSERVER
STAT LINK NODE <nodeID>	Display the link information status of the specified node. Where <nodeID> = a number from 0 - 9999. **Note:** The nodeID identifies the node number assigned to a group of Voice Gateway Media Cards and Signaling Server equipment.
STAT LINK SRV <serverType>	Display the link information status of the servers for the specified server type. Where <serverType> is: • ITGP (ITG Pentium) • SMC (Media Card) • SS (Signaling Server)
STAT SERV APP <applicationType>	Display the link information status of the server for the specified application.

Command	Description
	Where <applicationType> is: • LTPS (Line TPS) • VGW (Voice Gateway) • H323 (H.323 Virtual Trunk) • GK (GateKeeper) • SIP (Session Initiated Protocol) • MC32S = 32 port Mindspeed VGMC • SLG (SIP Line Gateway)
`STAT SERV IP <IP address>`	Display the link information status of the server for the specified IP address, or IP addresses contained in the specified sub-net. Where <IP address> = the ELAN IP address of the Signaling Server or Voice Gateway Media Card. **Note:** The IP address can be in full or partial IP address format (e.g., "10.11.12.13" or "10.11"). `
`STAT SERV NAME <hostName>`	Display the link information status of the servers based on the supplied host name. Where <hostname> = MAINSERVER.
`STAT SERV NODE <nodeID>`	Display the link information status of the specified node. Where <nodeID> = a number from 0 - 9999 identifying the node number assigned to a group of Voice Gateway Media Cards and Signaling Server equipment.
`STAT SERV TYPE <serverType>`	Display the server information of the specified server type. Where <serverType> is: • ITGP (ITG Pentium) • SMC (Media Card) • SS (Signaling Server)
`STAT SS`	Display the server information of the specified Signaling Server.
`STAT ZBR [<Zone>]`	Display status of branch office zones (displays which local dialing).

Command	Description
`STAT ZONE [<Zone>]`	Display zone status table.
`STIP ACF`	Displays status for all ACF calls.
`STIP ACF <status>`	Displays Active Call Failover (ACF) information.
`STIP DTLS <Node> <Connection_Type> <DTLS_Capability>`	Display IP Phones based on signaling encryption related values, namely the type of connection currently in use by each IP Phone and their capability to make DTLS connections. Where: • <Node> = the node ID of the node the subject IP phones belong to, or “ALL” to omit node-based filtering • <Connection_Type> = type of signaling encryption used - INSECURE = no signaling encryption - SECURE” = USec or DTLS - DTLS = DTLS - USEC = UNIStim Security - ALL = all encryption types • <DTLS_Capability> = capability to make DTLS connections - YES = able to make DTLS connections - NO = not able to make DTLS connections - ALL = both capabilities
`STIP HOSTIP <IP address>`	Display information contained in the resource locator module table corresponding to the specified HOSTIP address, or HOSTIP addresses contained in the specified sub-net. Where <IP address> = the ELAN IP address of the Signaling Server or Voice Gateway Media Card. **Note:** IP address can be in full or partial IP address format. For example, "10.11.12.13", or "10.11".

Command	Description
STIP NODE <nodeID>	Display information contained in the resource locator module table corresponding to the specified node ID. Where <nodeID> = a number from 0 - 9999 identifying the node number assigned to a group of Voice Gateway Media Cards and Signaling Server equipment.
STIP SIPLUA	Display SIP Line Services TNs with the specified User Agent string.
STIP TERMIP <IP address>	Display information contained in the resource locator module table corresponding to the specified TERMIP address, or TERMIP addresses contained in the specified sub-net. Where <IP address> = the TLAN IP address of the IP Phone or Voice Gateway Media Card. **Note:** IP address can be in full or partial IP address format. For example, "10.11.12.13", or "10.11".
STIP TN l s c u	Display the resource locator module information for the specified TN, or group of TNs, as denoted by the l s c u and cu parameters. **Note:** All codecs configured for the specified TN are listed in the format - <codec standard> and <bandwidth used for it>: CODEC(BW): G711a noVAD(1904), G711u noVAD(1904). The exact value of G.711 20ms codec BW usage is 190400 bps (or 190.4 kbps). However, the configured zone BW limit in the zone table is measured and configured in ‘kbps‘. The zone BW usage for a single call is counted in ‘kbps‘ and only in integer values. Zone BW usage should be readable. The STIP commands in LD 117 take BW value for IP codecs from the RLM table. RLM table stores the exact BW value and in the following format - 190400 bps divided to 100.
STIP TYPE <aaa>	Display the resource locator module information for the specified TN type. Where <aaa> is:

Command	Description
	• IP Phone type: - 1110 - 1120 - 1130 - 1140 - 1145 - 1150 - 1160 - 1210 - 1220 - 1230 - 2001 - 2002 - 2004 - 2007 - 2033 - 2050 - 2210 - 2211 - 2212 - MVC2050 • ISET = all IP Phones • VGW = Voice Gateway resources • IPTI = Virtual Trunk and IP Trunks **Note:** Up to 3 types can be specified.
`STIP ZONE <zone>`	Display the resource locator module information for the specified zone number, or range of zones. Where <zone> = any valid zone number (0 - 8000) in the system. `UPDATE DBS`
`UPDATE DBS`	Rebuild INET database and download to all Expansion Cabinets (update network database).

Command	Description
	Note: This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer. **Note:** To apply Network Time Protocol configuration to all system elements, ensure the configuration is done using Element Manager. CLI commands only configure the Call Server, and may lead to inconsistent NTP operation at the system level.

NTP Command descriptions

Note:
NTP commands are blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.

Note:
To apply Network Time Protocol configuration to all system elements, ensure the configuration is done using Element Manager. CLI commands only configure the Call Server, and may lead to inconsistent NTP operation at the system level.

Command	Comment
CHG NTP IPADDR	Configure the IP addresses for the Primary and/or Secondary NTP Servers.
CHG NTP THRESH	Configure the 3 NTP threshold levels (Minimum, Warning, Maximum).
CHG NTP SECURE	Configure the parameters used by the Primary and/or Secondary NTP servers in secure mode of operation.
CHG NTP AUTHMODE	Configure the security mode for the Primary, Secondary, or both, NTP servers.
CHG NTP TIMEINT	Configure both the time interval for background NTP synchronization and the time offset from other background routines.

Command	Comment
CHG UTCOFFSET	Configure the time offset (from UTC) for the local time zone.
ENL NTP	Enable NTP.
DIS NTP	Disable NTP.
STAT NTP	Check Status of NTP.
SYNC NTP	Synchronize NTP servers manually or in background mode.
STOP NTP BACKGROUND	Stop background synchronization from running.
PRT NTP	Display the current configuration parameters of NTP.

Alphabetical list of Administration commands

The commands listed below use the following general structure (where "=>" is the command prompt):

=> COMMAND OBJECT [(FIELD1 value) (FIELD 2 value)... (FIELDx value)]

In the following table, COMMANDS and OBJECTS are in bold typeface and fields are in regular typeface. Fields enclosed in brackets ( ) are default values.

Command	Description	Pack/Rel
`PRT BKPR ALL`	Administer Accounts. **Note:** This prompt is available only when adding/modifying Level 2 (PWD2) user. Allow TM system restore functionality for one usage.	basic-5.00
`BANNERLOAD aa...a`	Login Banner. Input terminated with \n OR \r\n. Restricted to: • 20 lines • Up to 80 characters per line • characters “a-z”, “A-Z”, ”0-9”, “,<.>/?;:’”[{]}‘~!@#$%^&*()_-+=|\”	basic-5.00

Command	Description	Pack/Rel
	Note: Available to users with the SEC_ADMIN privilege loads the contents from the /u/pub/ banner.txt for use as the system login banner An EDD is required to force all peripheral devices (SS/IPMG/ VGMC/Inactive Core) to update their login banners.	
`BANNER LOAD`	Load customized banner from banner.txt into memory.	
`BANNER RESET`	Reset banner contents with default value. **Note:** Available to users with the SEC_ADMIN privilege An EDD is required to force all peripheral devices (SS/IPMG/ VGMC/Inactive Core) to update their login banners.	basic-5.00
`BANNER SHOW`	Retrieves and displays the customized banner text from memory.	basic-5.00
`BROWSE SEL`	Browse system event log by lines or string	
`BROWSE SEL UP n`	Browse up n # of lines in System Event List (SEL).	
`BROWSE SEL DOWN n`	Browse down n # of lines in SEL.	
`BROWSE SEL TOP`	Browse to top of SEL.	
`BROWSE SEL BOT`	Browse to bottom of SEL.	
`BROWSE SEL FIND xxx`	Browse forward to find string xxx in SEL.	

Command	Description	Pack/Rel
BROWSE SEL BFIND xxx		
	Browse backward to find string xxx in SEL.	
BYRANGE		
	Return range of entries from embedded command	
CHG ADMIN_COMM n aa...a		basic-4.00
	Change SNMP community string for a given admin. group, where: • n = a number from 1 to 3 • aa...a = a string with a maximum length of 32 characters, where: - Default(1) = admingroup1 * - Default(2) = admingroup2 * - Default(3) = admingroup3 * * = case-sensitive These communities are used for accessing different SNMP objects on the Call Server, Signaling Servers, Voice Gateway Media Cards and Media Gateway Controllers.	
	In CS 1000 Release 6.0, if administration group community strings are added or modified in LD117, they are stored in an "OVLY 117 Configuration" area pending activation. When the SYNC SNMPCONF command is executed, the "OVLY 117 Configuration" changes are activated and become part of the "ACTIVE Configuration" on the system.	basic-6.00
CHG APPSRV		
	Change the IP address of the application server for PD.	
CHG BKPR xxx a...a b...b yy		grprim-4.00
	Change a Backup Rule, where: • xxx = Backup Rule number ID = (1)-100. Currently, only one rule is required for replication to the secondary system • a...a = SCS, rule type that allows direct replication to another system	

Command	Description	Pack/Rel
	• b...b = ELAN IP address of the destination system • yy = (2)-10, the number of database versions to save on the destination system	
`CHG BKPR <rule number1-100> FMD [<N of versions>] [<name>]`	Change backup rule to Fixed Media Device (FMD), where: • rule number = 1-100, Up to 100 rules can be defined. Each rule is a pattern that can be further used. FMD rules can be used by the backup schedules or for manual backup and restore operation (BKR/RSR commands activated from LD 43). • FMD = mnemonic for this rule type • N of versions = (1)-10 number of incremental backup data versions preserved on the local removable media device • name = rule name, where: text of up to 30 characters without white spaces is allowed **Note:** The <name> parameter is also added as optional when defining a new backup rule with SCS type (introduced in CS 1000 Release 4.0 Geographic Redundancy).	basic-4.50
`CHG BKPR <rule number1-100> FTP <IP addr> <login><pwd> <path> [<N of versions1-10>] [<name>]`	Change backup rule to an external FTP server, where: • <rule number> = 1-100, Up to 100 rules can be defined. Each rule is a pattern that can be further used. These rules can be used by the Geographic Redundancy Database Replication Control (GRDRC block as defined in LD-117), by the Backup Schedules for manual backup/restore operation (BKR/RSR commands activated from Ovl.43). • FTP = mnemonic for this rule type • IP addr = IP address of the FTP server to be accessed for storing (Backup) or retrieving (Restore) backup data • login = login name to access the FTP server, up to 32 characters • pwd = login password to access the FTP server, up to 32 characters	basic-4.50

Command	Description	Pack/Rel
	• path = path on the FTP server where the backup data file (or files for incremental versions) is located, up to 64 characters • N of versions = (1)-10 number of incremental backup data versions preserved on the FTP server • name = rule name, where: text of up to 30 characters without white spaces is allowed **Note:** The only backup rule type which can be referenced from GRDRC is SCS. **Note:** The <name> parameter is added as optional when defining a new backup rule with SCS type introduced in CS 1000 Release 4.0 Geographic Redundancy.	
`CHG BKPR <rule number1-100> RMD [<N of versions>] [<name>]`	Change backup rule to an Removable Media Device (RMD), where: • rule number = 1-100, Up to 100 rules can be defined. Each rule is a pattern that can be further used. RMD rules can be used by the backup schedules or for manual backup and restore operation (BKR/RSR commands activated from LD 43). • RMD = mnemonic for this rule type • N of versions = (1)-10 number of incremental backup data versions preserved on the local removable media device • name = rule name, where: text of up to 30 characters without white spaces is allowed **Note:** The <name> parameter is also added as optional when defining a new backup rule with SCS type (introduced in CS 1000 Release 4.0 Geographic Redundancy).	basic-4.50
`CHG BKPS <schedule number 1-10> <Rule for BKUP> <FREQ> <DAY> <HOUR>`	Change a backup schedule, where:	basic-4.50

Command	Description	Pack/Rel
	• Rule for BKUP = number of the backup rule for scheduled backup operation • FREQ = M/W/(D)/A - defines how often the scheduled backup takes place, where: - M = monthly - W = weekly - D = daily - A = automatically immediately after every EDD operation activated. There cannot be more than 1 schedule defined where FREQ = A **Note:** When FREQ = D, the next parameter is HOUR DAY = day of the week, applicable when FREQ = W or FREQ = M, where: - (SU) = Sunday - MO = Monday - TU = Tuesday - WE = Wednesday - TH = Thursaday - FR = Friday - SA = Saturday - (1)- 31 **Note:** When FREQ = M and the day specified is greater than the number of days in the current month, the backup takes place on the last day of the current month. HOUR = 0-(3)-23 **Note:** This rule type is not allowed if the GRPRIM/GRSEC package is equipped and the rule is used in GRDRC.	
`CHG CACVT <Zone> <1-(48)-255>`	Change the CAC record validity time interval in hours for CAC, where:	zcac-4.50

Command	Description	Pack/Rel
	• Zone = 0–255 • Zone = 0–8000 • 1-(48)-255 = interval in hours, default value is 48.	basic-7.0 0
`CHG CD <Zone> <1-(50)-100>`		zcac-4.5 0
	Change the CD coefficient for CAC on the particular zone, in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone, where: • Zone = 0–255 • Zone = 0–8000 • 1-(50)-100 = CD coefficient, default value is 50.	zcac-7.0 0
`CHG CJ <Zone> <1-(50)-100>`		zcac-4.5 0
	Change the CJ coefficient for CAC on the particular zone, in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone, where: • Zone = 0–255 • Zone = 0–8000 • 1-(50)-100 = jitter coefficient, default value is 50.	zcac-7.0 0
`CHG CPL <Zone> <1-(50)-100>`		zcac-4.5 0
	Change the CPL coefficient for CAC on the particular zone, in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone, where: • Zone = 0–255 • Zone = 0–8000 • 1-(50)-100 = CPL coefficient, default value is 50.	zcac-7.0 0
`CHG CQOS <Zone> <1-(50)-100>`		zcac-4.5 0
	Change the CQoS coefficient in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone, where:	

Command	Description	Pack/Rel
	• Zone = 0–255 • Zone = 0–8000 • 1-(50)-100 = QoS coefficient	zcac-7.00
CHG CQTH	Change the QoS warning and unacceptable thresholds on a per call basis	
CHG CQUTH <UnacpJitter> <UnacpLatency> <UnacpPacketLoss> <UnacpRFactor>	Change VQ Unacceptable thresholds on a per call basis, where: • UnacpJitter = 5-(40)-500 msec • UnacpLatency = 5-(100)-500 msec • UnacpPacketLoss = 5-(70)-250 in units [1/10 of a percent] For example, 10 means 1% • UnacpRFactor = 20-(60)-94 **Note:** Changes to threshold values are not propagated to the Signaling Server or the Voice Gateway Media card until a data dump is performed.	pvqm-4.0
CHG CQWTH <WarnJitter> <WarnLatency> <WarnPacketLoss> <WarnRFactor>	Change VQ Warning thresholds on a per call basis, where: • WarnJitter = 5-(20)-200 msec • WarnLatency = 5-(40)-100 msec • WarnPacketLoss = 5-(20)-100 in units [1/10 of a percent] For example, 10 means 1% • WarnRFactor = 20-(65)-94 **Note:** Changes to threshold values are not propagated to the Signaling Server or the Voice Gateway Media card until a data dump is performed.	pvqm-4.0
CHG CR <Zone> <1-(50)-100>		zcac-4.50

Command	Description	Pack/Rel
	Change the Cr co-efficient in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone, where: • Zone = 0–255 • Zone = 0–8000 • 1-(50)-100 = Cr coefficient	zcac-7.00
`CHG EDT`	Enable/disable the use of Event Default Table (EDT).	
`CHG EDT NORMAL`	Use Event Default Table (EDT) default severities.	alrm_filter-21
`CHG EDT INFO`	Override EDT; use INFO as the default severity for all events except those specified in Event Preference Table (EPT).	alrm_filter-21
`CHG EDT MINOR`	Override EDT; use MINOR as the default severity for all events except those specified in Event Preference Table (EPT)	alrm_filter-21
`CHG ELNK ACTIVE hostname`	Set system active Ethernet interface IP address (set active ELAN IP address). **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
`CHG ELNK INACTIVE hostname`	Set system inactive Ethernet interface IP address (set inactive ELAN IP address) **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	

Command	Description	Pack/Rel
CHG EPT aa... a INFO x	Change an Event Preference Table (EPT) entry to Information severity, where: • aa... a = an event class with an event number (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your CHG SUPPRESS entry	alrm_filter-21
CHG EPT aa... a EDT x	Change EPT to NT-defined severity from EDT, where: • aa... a = an event class with an event number (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your CHG SUPPRESS entry	alrm_filter-21
CHG EPT aa... a MAJOR x	Change an EPT entry to Major severity, where: • aa... a = an event class with an event number (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your CHG SUPPRESS entry	alrm_filter-21
CHG EPT aa... a MINOR x	Change an EPT entry to Minor severity, where: • aa... a = an event class with an event number (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your CHG SUPPRESS entry	alrm_filter-21
CHG EPT aa... a CRITICAL x	Change an EPT entry to Critical severity, where:	alrm_filter-21

Command	Description	Pack/Rel
	• aa... a = an event class with an event number (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your CHG SUPPRESS entry	
`CHG ERL <erl> [<RT_RLI> <route_rli> <ac> <prepend> <staticELIN> <osdn>]`		basic-5.00
	Change an Emergency Response Location (ERL) table entry, where: • <erl> = Emergency Response Location (ERL) identifier Number in the range 1-65535. • <RT_RLI> = token identifying the emergency call routing mechanism for the ERL - RT = by route number - RLI = by Route Line Index • <route_rli> = number of route or route line index (as indicated by <RT_RLI> token) - route number = as specified in LD 16 - route line index number = as specified in LD 86 • <ac> = access code, as specified in LD 90 • <prepend> = prepended routing digits for emergency calls • <staticELIN> = static Emergency Location Identification Number (ELIN) • <osdn> = On-Site Notification DN To skip a field and set it to blank, use either a NULL or NONE token in its place. Any fields not specified at the end of the command are set to blank, as if you entered NULL or NONE for each one.	
`CHG ERLLOC <ERL#> <Location Description>`		basic-5.00
	Assign a Location Description to an ERL.	
`CHG ERLSITE <ERL#> <Site Name>`		basic-5.00
	Assign a Site Name to an ERL.	
`CHG ES1 <Echo Server IP Address> <Echo Server Port>`		basic-4.00

Command	Description	Pack/Rel
	Change the Echo Server 1 IP address and port number, where: • Echo Server 1 IP Address = (0.0.0.0) • Echo Server 1 Port number = (10000) **Note:** Echo Server 1 IP address uses the TLAN IP address of the LTPS card.	
`CHG ES2 <Echo Server IP Address> <Echo Server Port>`		basic-4.00
	Change the Echo Server 2 IP address and port number, where: • Echo Server IP Address = (0.0.0.0) • Echo Server Port = (10000) **Note:** Echo Server 2 default IP address uses the node IP address on the node's master card.	
`CHG FMT_OUTPUT OFF`		alrm_filter-21
	Turn off formatted output	
`CHG FMT_OUTPUT ON`		alrm_filter-21
	Turn on formatted output	
`CHG GRDRC xxx aaa yyy bbb ccc`		grprim-4.00
	Change current Geographic Redundancy Data Replication Control (GRDRC) block, where: • xxx = Backup Rule number. • aaa = how the automatic database replication to the destination system occurs. Geographic Redundancy requires that this parameter be configured as SCHD: - SCHD - according to defined backup schedule - (IMM) - immediately after any data dump operation - MIDN - after midnight data dump only - NO - not allowed	

Command	Description	Pack/Rel
	• yyy = Backup Rule number used for the restore operation on the secondary system. If no rule number is entered, then this points to the <BKUP rule>. • bbb = (YES) NO, Allow or deny automatic restore operation on the secondary system • ccc = (YES) NO, Allow or deny automatic sysload after successful automatic restore on the secondary system **Note:** ccc = YES is allowed only if bbb = YES	
`CHG GRNS <FREQ><DAY><HOUR><MINUTE>[<DELAY>]`	Change GR N-way backup schedules, where: • FREQ = defines how often the backup takes place, where: - M = monthly - W = weekly - D = daily • DAY = day of the week, applicable when FREQ = W or FREQ = M, where: - (SU) = Sunday - MO = Monday - TU = Tuesday - WE = Wednesday - TH = Thursday - FR = Friday - SA = Saturday - (1)-31 When FREQ = D, the next parameter is HOUR. • HOUR = 0-(3)-23 • MINUTE = (0)-59 • DELAY = (3)-60 The interval in minutes between two consecutively scheduled backups. The system scans for backup rules of SCS type and modifies a BKPS for each of them and adjusts the start times according to the specified delayed value.	basic-5.00

Command	Description	Pack/Rel
`CHG GRSC xxx yyy zzz a..a`	Change current Geographic Redundancy State Control (GRSC) block, where: • xxx = (1)-10% x (Basic IP User License + IP User License), the number of IP phones that must register on the secondary system for the system to escalate to the ACTIVATING state • yyy = (5)-600, Short Term Failure Timer in minutes • zzz = (5)-180, Failure Clearance Timer in minutes • a..a = (AUTO) MAN, Secondary system Deactivation Mode, where: - (AUTO) = Automatic - MAN = Manual	grprim-4.00
`CHG HSP_MASK <subnet mask>`	Modify the manually-configured HSP subnet mask, if it exists; otherwise, the subnet mask to the Call Server is added. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	basic-4.50
`CHG IPR`	Change current 100BaseT IP configuration data for IPMG.	
`CHG IPR x mac ip mask`	Change the IP connectivity configuration data associated with the IP (Intelligent Peripheral) Expansion cabinet end of the specified port, where: • x = 1-4, port number of the main cabinet to which the expansion cabinet is connected • mac = xx:xx:xx:xx:xx:xx, MAC address obtained from the sticker on the IP daughterboard mounted on the IP Expansion SSC, where: x is a hexidecimal digit in the range 0-F	

Command	Description	Pack/Rel
	• ip = x.x.x.x, Internet Protocol address, where: x is an integer in the range 0–255 • mask = x.x.x.x , subnet mask, where: x is an interger in the range 0–255	
CHG IPM		
	Change current 100BaseT IP configuration data for Call Server.	
CHG IPM x ip mask		
	Change the IP connectivity configuration associated with the main cabinet end of the specified port, where: • x = 1-4, port number of the main cabinet to which the expansion cabinet is connected • ip = x.x.x.x, Internet Protocol address, where: x is an integer in the range 0–255 • mask = x.x.x.x, subnet mask, where: x is an interger in the range 0–255	
CHG L3ELAN x ACTIVE <address>		basic-5.0 0
	Define physical active ELAN address: Where: • x = 0 OR 1 Core • Address = nnn.nnn.nnn.nnn	
CHG L3GW x <address>		basic-5.0 0
	Define physical ELAN default gateway address: Where: • x = 0 OR 1 Core • Address = nnn.nnn.nnn.nnn	
CHG L3HSP <side> <address>		basic-5.0 0
	Change Layer 3 Hot Standby Protocol of VPN Router Where: • Side = 0 OR 1 Core • Address = nnn.nnn.nnn.nnn	

Command	Description	Pack/Rel
CHG L3HSPGW <side> <address>	Change Layer 3 Hot Standby Gateway of VPN Router Where: • Side = 0 OR 1 Core • Address = nnn.nnn.nnn.nnn	basic-5.00
CHG L3HSPMASK <side> <mask>	Change Layer 3 Hot Standby Mask of VPN Router Where: • Side = 0 OR 1 Core • Mask = nnn.nnn.nnn.nnn	basic-5.00
CHG L3MASK <side> <mask>	Change the mask of the side specific ELAN port. Where: • Side = 0 OR 1 Core • Mask = nnn.nnn.nnn.nnn	basic-5.00
CHG L3PRIV active | inactive <address>	Define the IP address of the virtual ACTIVE / INACTIVE ELAN: Where: Address = nnn.nnn.nnn.nnn	basic-5.00
CHG LCL	Change the Local Core Location Loop and Shelf values (Applicable only to CP PM and Linux CS).	
CHG LDAPSYNC <ldapsync> [<timeOfDay> [<ldapserver> <userid> < password> [<security> [<secure port> [insecure port>]]]]]	Enable/disable the scheduled synchronization of the Unicode Name Directory data with the CND LDAP server data, or change the parameters for the scheduled synchronization task. Where: • <ldapsync> = disable/enable scheduled synchronization of the Unicode Name Directory data with the CND LDAP server data - 0 = disable	basic-6.00

Command	Description	Pack/Rel
	- 1 = enable • <timeOfDay> = the time of day for scheduled LDAP synchronization Format = hh:mm • <ldapserver> = IP address or FQDN of the CND LDAP server • <userid> = username required for access to the CND LDAP server • <password> = password required for access to the CND LDAP server • <security> = enable/disable secure SSL connection to the CND LDAP server • <secure port> = port used for secure SSL connection to CND LDAP server. Default port = 636. • <insecure port> = port used for insecure connection to CND LDAP server. Default port = 389. **Note:** <userid> and <password> must always be specified as a pair.	
`CHG MASK nnn.nnn.nnn.nnn`	Change subnet mask. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
`CHG NAV_SITE aa... a`	Change the navigation site name (MyCity, for example), where: • aa...a = a string with maximum length of 32 characters • default = Navigation Site Name **Note:** Use a single X to clear the field. In CS 1000 Release 6.0, if the navigation site name is modified in LD117, it is stored in an "OVLY 117 Configuration" area	basic-4.00 basic-6.00

Command	Description	Pack/Rel
	pending activation. When the SYNC SNMPCONF command is executed, the "OVLY 117 Configuration" changes are activated and become part of the "ACTIVE Configuration" on the system.	
`CHG NBWMM IP`	Set the IP address of the Primary NBWM Master.	
`CHG NBWMM STATE`	Change the IP Peer System state.	
`CHG NBWMMA IP`	Set the IP address of Alternate NBWM Master.	
`CHG NDAPP <ndAppValue> [<ndLkupTimer>]`	Enable/disable the Name Directory Application. Where: • <ndAppValue> = 0, 1, OFF, ON - 0 or OFF = disabled - 1 or ON = enabled • <ndLkupTimer> = 500-10000 If not specified, a default value of 3000 msec is used.	basic-6.00
`CHG NKT`	Change NAT Mapping Keep Alive time-out setting of port mapping for devices behind a NAT router, where: time out setting = 0-(30)-60 seconds	basic-4.00
`CHG NTP AUTHMODE <Secure | Insecure> <Primary | Secondary | All>`	Configure the security mode for the Primary, Secondary, or both, NTP servers. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	basic-5.00

Command	Description	Pack/Rel
CHG NTP IPADDR <primary_ip_addr> <secondary_ip_addr>	Configure the IP addresses for the Primary and Secondary NTP Servers. **Note:** When you are configuring the IP address for the secondary NTP server, enter the IP address of the primary NTP server, followed by the IP address of the secondary NTP server. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	basic-5.00
CHG NTP MODE CS	Configure Router as the mode of communication between the NTP server and the CS. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	basic-5.00
CHG NTP MODE SS	Configure Signaling Server as the mode of communication between the NTP server and the CS. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	basic-5.00
CHG NTP SECURE <primary_ip_add> <secondary_ip_addr> <key_id>	Configure the parameters used by the Primary and/or Secondary NTP servers in secure mode of operation. Where: • <primary_ip_add> = IP address of primary NTP server • <secondary_ip_addr> = IP address of secondary NTP server • <key_id> = private key with values = 1 - 4294967295.	basic-5.00

Command	Description	Pack/Rel
	The system prompts for the private key if not entered. **Note:** For security reasons, the private key does not show in the command line as you enter it. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	
`CHG NTP THRESH <Minimum> <Warning> <Maximum>`	Configure the 3 NTP threshold levels. Where: • <Minimum> = (0)-5 seconds • <Warning> = (6)-15 seconds • <Maximum> = (16)>15 seconds **Note:** Enter values for all three threshold levels when you use this command. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	basic-5.00
`CHG NTP TIMEINT <time interval in hours> <offset in minutes>`	Configure both the time interval for background synchronization and the offset from other background routines. Where: • <time interval in hours> = 1, 2, 6, 12, (24), 30 • <offset in minutes> = 15, (30), 45 **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	basic-5.00

Command	Description	Pack/Rel
CHG NUMZONE <numbering zone> <site_prefix> <country_code> <npa> <ac1> <ac2> <natc> <intc> <dac> <ttbl>	Change the parameters of a ZBD numbering zone. Where: • <numbering zone> = new numbering zone number A number from 1-1023. • ZBD zone parameters: - <site_prefix> = site prefix A number from 0-9999. - <country_code> = country code A number from 0-9999. - <npa> = area code (used for dialing through ZFDP) A number from 0-9999. - <ac1> = trunk access code 1 A number from 0-99. - <ac2> = trunk access code 2 A number from 0-99. - <natc> = national dial code A number from 0-9999. - <intc> = international dial code A number from 0-9999. - <dac> = flag to delete NPA for a local subscriber call A number from (0)-1. - <ttbl> = tone table A number from (0)-32.	zbd-6.00
CHG NZDES <numbering zone> <description>	Change the description of a ZBD numbering zone. Where: • <numbering zone> = 1-1023 • <description> = 1-128 characters Description of numbering zone.	zbd-6.00
CHG PDBAK	Change parameters for remote backup of PD	
CHG PDV	Change PDV value in milliseconds	

Command	Description	Pack/Rel
CHG PPP LOCAL hostname		
	Set Meridian 1 local Point-to-point Protocol interface IP address	
CHG PPP REMOTE hostname		
	Set Meridian 1 remote Point-to-point Protocol interface IP address	
CHG PTM 0-60		
	Change Point-to-point Protocol idle timer to specified value, where: 0-60 = value in minutes	
CHG RCL		
	Change the Remote Core Location Loop and Shelf values (Applicable only to CP PM and Linux CS).	
CHG SELSIZE 5-(500)-2000		
	Change System Event List Size, where: 5-(500)-2000 = number of events in SEL	
CHG SNMP_SYSCONTACT aa... a		basic-4.00
	Change the contact person name for this system element (machine).	
	Where aa...a = a string with a maximum length of 100 characters.	basic-4.00
	Default = "System Contact". **Note:** Use a single X to clear the field.	
CHG SNMP_SYSLOC aa...a		basic-4.00
	Change the defined physical location for this system element (machine).	
	Where aa...a = a string with a maximum length of 100 characters.	basic-4.00
	Default = "System Location".	

Command	Description	Pack/Rel
	Note: Use a single X to clear the field.	
`CHG SNMP_SYSNAME aa...a`		basic-4.00
	Change the system name assigned to this system element (machine).	
	Where aa...a = a system name string with a maximum length of 100 characters.	basic-4.00
	can include a %hostname% variable that allows the system to configure the physical hostname as a component of the system element name	basic-5.50
	Default = "System Name".	
	Note: Use a single X to clear the field.	
`CHG SQOS <SamplePeriod> <SampleRateWindow> <MinSampleCnt>`		pvqm-4.0
	Change VQ sampling parameters, where: • SamplePeriod = 5-(30)-60 seconds • SampleRateWindow = 60-(300)-3600 seconds • MinSampleCnt = 50-(100)-1000	
`CHG SUBNET <IP Address> <Mask> <ERL> <ECL> "<Location Description>"`		basic-5.00
	Change a subnet entry where: • IP address = nnn.nnn.nnn.nnn • Mask = nnn.nnn.nnn.nnn • ERL and ECL = 0-65535 • Location Description = 20 alphanumeric characters withn quotation marks.	
	Note: Only the location fields (ERL, ECL, and Location Description) can be changed.	

Command	Description	Pack/Rel
CHG SUPPRESS 5-(15)-127	Change global suppress for events, where: 5-(15)-127 = number of occurrences before event is suppressed	alrm_filter-21
CHG SUPPRESS_ALARM [n]	Changes the minimum alarm severity threshold of the alarms that are sent. Where [n] is: • 0 = All • 1 = Minor • 2 = Major • 3 = Critical	basic-4.00
SYNC SNMPCONF	Update the "ACTIVE Configuration" (current) SNMP parameters on the CS with "OVLY 117 Configuration" SNMP parameters, and propagate the updated SNMP parameters to all system elements that have an established pbxlink with the CS.	basic-6.00
SYNC SYS	Propagates Dbconfig and QOS parameters on the CS to all system elements that have an established pbxlink with the CS.	basic-5.00
CHG SYSMGMT_TRAP_COMM <aaa...a>	Configure the SNMP community string	basic-5.00
CHG SYSMGMT_RD_COMM n aa...a	Change the system management read-only community name string, where: aa...a = a string with a maximum length of 32 characters	basic-4.00
CHG SYSMGMT_WR_COMM n aa...a		basic-4.00

Command	Description	Pack/Rel
	Change the system management read / write community name string, where: aa...a = a string with a maximum length of 32 characters	
`CHG TIMER (1)-60`		alrm_filter-21
	Change global timer window length, where: (1)-60 = time in minutes **Note:** SeeGlobal window timer length on page 364 for more information.	
`CHG UTCOFFSET <Time Offset>>`		basic-5.00
	Configure the time offset (from UTC) for the local time zone. Where <Time Offset> = +/-hh:mm (+00:00). **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
`CHG VPNKEY <key>`		basic-5.00
	Define the VPN pre-shared key. Where: key = 8 to 64 Alphanumeric characters	
`CHG VPNMASK <mask>`		basic-5.00
	Change the VPN mask = nnn.nnn.nnn.nnn	
`CHG VPNNET <ip address>`		basic-5.00
	Change the VPN network IP address = nnn.nnn.nnn.nnn	
`CHG VPNROUTER <side> <address type> <address>`		basic-5.00
	Configure interface of VPN Router Where:	

Command	Description	Pack/Rel
	• Side = 0 / 1 (number of the core) • Address type = ‘PUBLIC’ / ‘PRIVATE’ VPN Router interface • Address = nnn.nnn.nnn.nnn	
CHG ZACB <Zone>[ALL] [<AC1...AC2> <AC1...AC2>]	Define the access codes used to modify local calls in the branch office zone, where: • ALL = both AC1 and AC2 receive digit manipulation and no re-translation occurs • AC1 = the first Access Code parameter defines which NARS Access Code to consider as the source of local calls • AC2 = the second Access Code parameter defines which NARS Access Code to send the modified number to for retranslation. **Note:** If NARS is configured as recommended in the NTPs, this would be AC2 for local call and AC1 for retranslation.	
CHG ZALT <zone> <ALTPrefix> [<All_calls>]	Change Alternate Prefix number for zone, where: • zone = 0–255 • Zone = 0–8000 • ALTPrefix = digit string of up to 7 digits that is added to the start of dialed number if the call do not be routed through the WAN due to lack of bandwidth, poor QoS or feature is configured for all calls. • All_calls = Allow or Deny Alternative Routing for all calls, where: - (NO) = deny - YES = allow	basic-4.50 basic-7.00
CHG ZAST <zone> [<AlarmSuppressTime>]	Changes ACR settings for particular zone, where:	basic-4.50

Command	Description	Pack/Rel
	• zone = 0–255 • Zone = 0–8000 • AlarmSuppressTime = 0-3600, time in seconds	basic-7.00
`CHG ZBRN <Zone> <a...a>`	Define a zone as a branch office zone, where: • Zone = 0–255 • Zone = 0–8000 • a...a = Yes or No	basic-7.00
`CHG ZDID <numbering zone> <matching string> <replacement string> [<description>]`	Change a ZBD numbering zone-based call translation table entry. Where: • <numbering zone> = 1-1023 • <matching string> = 1-16 digit “best match” numeric string Unique inside a numbering zone. • [<replacement string>] = string that replaces the matching string If <type> = SPN, CDP or ESDN, 1-16 numeric digits; if <type> = INTL, LOC, REG1, NPA, REG2 or NXX, 1-16 alphabetic characters. If <replacement string> is not specified, the matching string is deleted and not replaced. • <description> = 1-32 character textual description for the numbering zone-based call translation (ZDID) table entry If not specified, the ZDID table entry remains unchanged.	zbd-6.00
`CHG ZDES <Zone> <ZoneDescription>`	Assign a descriptive name to make the zone numbers more meaningful, where: • Zone = 0–255 • Zone = 0–8000 • ZoneDescription = descriptive name that is used only in the data display and status commands	basic-7.00
`CHG ZDP <Zone> <DialingCode1> <DialingCode2> <DialingCode3>`		

Command	Description	Pack/Rel
	Define the dialing plan for the branch office zone, where: • Zone = 0–255 • Zone = 0–8000 • DialingCode1 = Prefix, represents the access code for long distance or international access. In North America, it is "1" for long distance access and "011" for international access. Outside North America, it is "0" for national access and "00" for international access. • DialingCode2 = The country code or trunk code. Normally NPA when calling from within North America, and "1" when calling from outside North America. • DialingCode3 = Destination network code. Normally not used in North America. Outside North America, it is a combination of region, city, or district codes.	basic-7.00
`CHG ZDST <Zone> a...a <StartMonth> <StartWeek> <StartDay> <StartHour> <EndMonth> <EndWeek> <EndDay> <EndHour>`	Specifies whether the branch office zone observes daylight savings time, where: • Zone = 0–255 • Zone = 0–8000 • a...a = Yes or No, During daylight saving time, the clock automatically advances one hour forward. • StartMonth = start month of year (1-12) • StartWeek = start week in month (1-5) • StartDay = start day in week (1-7) • StartHour = start hour of day (1-23) of the start of DST • EndMonth = end month of year (1-12) • EndWeek = end week in month (1-5) • EndDay = end day in week (1-7) • EndHour = end hour of day (1-23) of the end of DST. **Note:** In North America, DST normally starts on the 1st Sunday in April at 2am and ends on the last Sunday in October at 2am. The digit 5 is the last week of the month irrespective of number of weeks this month. For example: StartWeek = start week in month (1-5) [1st-5th, 5 is the last week of the month]	basic-7.00

Command	Description	Pack/Rel
CHG ZESA <Zone> <ESARLI> <ESAPrefix> <ESALocator>	Defines the Emergency Services Access (ESA) parameters for the branch office zone. These parameters are used only if the ESA package is enabled, where: • Zone = 0–255 • Zone = 0–8000 • ESARLI = the route to use to send emergency calls to the branch office Gateway by way of the VTRK • ESAPrefix = a digit string of up to 15 digits that is added to the start of the ESDN before it is sent to the route indicated by the ESARLI. This allows the Gatekeeper to differentiate the different destinations for otherwise identical ESDN's • ESALocator = the DID phone number to be sent for use by the PSAP to locate the source of the emergency call	basic-7.00
CHG ZFDP <numbering zone> <matching string> <type> [<replacement string>] [LEN <max length>] ["<description>"]	Change a ZBD numbering zone-based flexible dialing plan table entry. Where: • <numbering zone> = 1-1023 • <matching string> = 1-16 digit “best match” numeric string Unique inside a numbering zone. • <type> = values specified in the LD 15 AC1 and AC2 prompts After stripping the matching string, save the CLID type and take the following actions depending on <type> specified: - If <type> = INTL (International E.164 number), insert AC1/AC2+replacement string. - If <type> = LOC (UDP Location Code), insert AC1/AC2+ replacement string. - If <type> = REG1 (Regional Level 1), insert AC1/AC2+ZCC +replacement string. - If <type> = NPA (North American NPA), insert AC1/AC2+1, then replacement string. - If <type> = REG2 (Regional Level 2), insert AC1/AC2+ZCC +ZNPA+replacement string - If <type> = NXX (North American NXX), insert AC1/AC2+ZCC+ZNPA+replacement string	zbd-6.00

Command	Description	Pack/Rel
	- If <type> = SPN (Special Number), insert AC1/ AC2+replacement string - If <type> = CDP (Coordinated Dial Plan), insert replacement string - If <type> = ESDN (Emergency Service DN), insert replacement string • [<replacement string>] = string that replaces the matching string If <type> = SPN, CDP or ESDN, 1-16 numeric digits; if <type> = INTL, LOC, REG1, NPA, REG2 or NXX, 1-16 alphabetic characters. If <replacement string> is not specified, the matching string is deleted and not replaced. • [LEN <max length>] = maximum number of dialed digits expected to match If not specified, default is to match digits for all multiple matches. • [<description>] = textual description of the numbering zone-based flexible dialing plan (ZFDP) table entry If not specified, the ZFDP table entry has no textual description.	
`CHG ZONE <ZoneNumber> <intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <a...a>` Change the parameters of an existing Zone, where: • ZoneNumber = 0–255 • Zone = 0–8000 • intraZoneBandwidth = Intrazone available bandwidth (0 to 0.1MBps) • intraZoneStrategy = BQ or BB, Intrazone preferred strategy (BQ for Best Quality or BB for best Bandwidth) • interZoneBandwidth = Interzone available bandwidth (0 to 0.1MBps) • interZoneStrategy = BQ or BB, Interzone perferred strategy ((BQ for Best Quality or BB for best Bandwidth) • a...a = type of zone, where: - (Shared) = current default zone type. The ethersets configured in shared zones use DSP resources configured in shared zones. If all of the shared zones' gateway		basic-7.0 0

Command	Description	Pack/Rel
	channels are used, the caller receives an overflow tone and the call is blocked. The order of channel selection for the gateway channels is: • channel from same zone as etherset is configured • any available channel from the shared zones' channels - Private = This zone type is introduced by IPL 3.0. DSP channels configured in a private zone are used only by ethersets which have also been configured for that private zone. If more DSP resources are required by these ethersets than what are available in the zone, DSPs from other zones is used. However, ethersets configured in shared zones cannot use the private zones' channels. The order of selection for the gateway channels is: • channel from same private zone as etherset is configured • any available channel from the pool of shared zones' channels	
`CHG ZONE <zoneNumber> <intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> [<zoneIntent> <zoneResourceType>]`	Change the parameters of an existing Zone. All parameters must be re-entered, where: • zoneNumber = 0–255 • Zone = 0–8000 • intraZoneBandwidth = 0-.1Mbps • intraZoneStrategy = intrazone preferred strategy, where: - BQ = Best Quality - BB = Best Bandwidth • interZoneBandwidth = 0-.1Mbps • interZoneStrategy = interzone preferred strategy, where: - BQ = Best Quality - BB = Best Bandwidth • zoneIntent = type of zone, where: - MO = Main Office zone - BMG = Branch Media Gateway zone	basic-4.50 basic-7.00

Command	Description	Pack/Rel
	- VTRK = Virtual Trunk zone • zoneResourceType = resource Intrazone preferred strategy, where: - (shared) = shared DSP channels - private = private DSP channels **Note:** With release 4.50 the zones that were described with BMG designator stay with BMG one, all the other zones are provided with the MO designator. It is possible to update ZoneIntent using CHG ZONE command.	
CHG ZPARM <numbering zone> <parameter name> <value>	Change the value of a ZBD numbering zone parameter. Where: • <numbering zone> = 1-1023 • <parameter name> = name of numbering zone parameter Where: - PREF = site prefix - CC = country code - NPA = area code (used for dialing through ZFDP) - AC1 = trunk access code 1 - AC2 = trunk access code 2 - NATC = national dial code - INTC = international dial code - DAC = flag to delete NPA for a local subscriber call - TTBL = tone table • <value> = new value for specified parameter - If <parameter name> = PREF, <value> = 0-9999. - If <parameter name> = CC, <value> = 0-9999. - If <parameter name> = NPA, <value> = 0-9999. - If <parameter name> = AC1, <value> = 0-99. - If <parameter name> = AC2, <value> = 0-99. - If <parameter name> = NATC, <value> = 0-9999. - If <parameter name> = INTC, <value> = 0-9999. - If <parameter name> = INTC, <value> = 0-9999.	zbd-6.00

Command	Description	Pack/Rel
	- If <parameter name> = DAC, <value> = (0)-1. - If <parameter name> = TTBL, <value> = (0)-32.	
CHG ZQNL <level>		pvqm-40
	Change the Notification Level for all zones, where: level = 0-(2)-4, where: - Level 0 = All voice quality alarms are suppressed. - Level 1 = Allow zone-based Unacceptable alarms. - Level 2 = Allow all level 1 alarms PLUS zone-based Warning alarms. - Level 3 = Allow all level 1 and 2 alarms PLUS per-call Unacceptable alarms. - Level 4 = Allow all level 1, 2, and 3 alarms PLUS per-call Warning alarms.	
CHG ZQNL <ZoneNumber> <level>		pvqm-40
	Change the Notification Level for the specified zone, where: • ZoneNumber = 0–255 • Zone = 0–8000 • level = 0-(2)-4	pvqm-7.00
CHG ZQRT <Zone> <1-100>		zcac-4.50
	Change ZQRT which is Response time increase by percentage. It is the amount by which the Sliding Maximum is increased for the identified zone, where: • Zone = 0–255 • Zone = 0–8000 • 1-(10)-100 = increase value in percentage	zcac-7.00
CHG ZQRTI <Zone> <1-120>		zcac-4.50
	Change the QoS Response Time Interval while alarms are not coming to increase the Sliding Maximum for the identified zone, where:	

Command	Description	Pack/Rel
	• Zone = 0–255 • Zone = 0–8000 • 1-(5)-120 = Interval in minutes	zcac-7.0 0
CHG ZQUAT <Zone> <1-99>		zcac-4.5 0
	Change the QoS Unacceptable Alarm Threshold value for the identified zone, where: • Zone = 0–255 • Zone = 0–8000 • 1-(75)-99 = threshold value **Note:** When the zone-to-zone QoS value transitions below this value, this alarm is presented. When the zone-to-zone QoS value transitions above this value, this alarm is presented as being deactivated. This value must be below the value of ZQWAT.	zcac-7.0 0
CHG ZQWAT <Zone> <1-99>		zcac-4.5 0
	Change the QoS Warning Alarm Threshold value for the identified zone, where: • Zone = 0–255 • Zone = 0–8000 • 1-(85)-99 = threshold value **Note:** When the zone-to-zone QoS value drops below this value, this alarm is presented. When the zone-to-zone QoS value transitions above this value, this alarm is reported as deactivated. The value for ZQWAT must be higher than the value of ZQUAT.	zcac-7.0 0
CHG ZQWTH <WarnJitter> <WarnLatency> <WarnPacketLoss> <WarnRFactor>		pvqm-4.0
	Change VQ Warning thresholds, where: • WarnJitter = 0-(20)-100% • WarnLatency = 0-(20)-100%	

Command	Description	Pack/Rel
	• WarnPacketLoss = 0-(20)-100% • WarnRFactor = 0-(20)-100% **Note:** Changes to threshold values are not propagated to the Signaling Server or the Voice Gateway Media card until a data dump is performed.	
`CHG ZQUTH <UnacpJitter> <UnacpLatency> <UnacpPacketLoss> <UnacpRFactor>`	Change VQ Unacceptable thresholds on a zone basis, where: • UnacpJitter = 0-(2)-100% • UnacpLatency = 0-(2)-100% • UnacpPacketLoss = 0-(2)-100% • UnacpRFactor = 0-(2)-100% **Note:** Changes to threshold values are not propagated to the Signaling Server or the Voice Gateway Media card until a data dump is performed.	pvqm-4.0
`CHG ZTDF <Zone> <TimeDifferenceFromHeadOffice>`	Specify the time difference between the Main Office and the branch office when both are not in Daylight Saving Time, where: • Zone = 0–255 • Zone = 0–8000 • TimeDifferenceFromHeadOffice = -1380 to 1380 minutes (Minus 23 hours to plus 23 hours), time difference in minutes	basic-7.00
`CLR CACR <Near Zone> {<Near VPNI>} {<Far Zone>} {<Far VPNI>}`	Clear zone-to-zone record for near (VPNI-Zone) per far (VPNI-Zone), where: • Near Zone = 0–255 • Near Zone = 0–8000 • Near VPNI = 1-16282, Virtual Private Network Identifier • Far Zone = 0–255	zcac-4.50 zcac-7.00 zcac-7.00

Command	Description	Pack/Rel
	• Far Zone = 0–8000 • Far VPNI = 1-16282, Virtual Private Network Identifier	
DIS SHELLS SECURE	Disables all secure shells in the system, includes SSH, SFTP, and SCP sessions. **Warning:** Disabling the shells causes telephony applications on external devices to stop communicating with the PBX. SFTP is required in regular operation of the CS 1000. Do not disable SFTP on VxWorks unless you have to troubleshoot a problem, if any.	basic-4.50
DIS SHELLS INSECURE	Disables all insecured shells in the system, includes TELNET, RLOGIN, and FTP sessions. **Warning:** Disabling the shells causes telephony applications on external devices to stop communicating with the PBX.	basic-4.50
DIS TRANSFERS INSECURE	Disable FTP (insecure File Transfer Protocol) on the system. Call server sends a related message through pbxLink to all connected devices and IPMG devices. **Note:** SFTP must be enabled. FTP and SFTP cannot both be disabled at the same time. **Note:** Command cannot be issued within 5 minutes of a previously issued ENL TRANSFERs or DIS TRANSFERS command.	basic-6.00
DIS TRANSFERS SECURE	Disable SFTP (secure File Transfer Protocol). Call server sends a related message through pbxLink to all connected devices and IPMG devices.	basic-6.00

Command	Description	Pack/Rel
	Important: SFTP is required in regular operation of the CS 1000. Do not disable SFTP on VxWorks unless you have to troubleshoot a problem, if any. **Note:** FTP must be enabled. FTP and SFTP cannot both be disabled at the same time. **Note:** Command cannot be issued within 5 minutes of a previously issued ENL TRANSFERs or DIS TRANSFERS command.	
`ECNT CARD`	Print all registered IP Phones with associated card.	basic-4.50
`ECNT CARD l s c [<customer>]`	Print the number of IP Phones registered, where: • l s c = loop, shelf, card • customer = customer number associated with this command **Note:** Partial TN are allowed	basic 4.50
`ECNT FW`	Print all registered IP Phones for each available firmware ID	basic-4.50
`ECNT FW <XX> [<A>] [<BB>] [<FF>]`	Print the number of IP Phones, where: • XX = firmware ID • A = major version designator • BB = minor version designator • FF = filter to apply on firmware version, where: - (==) = equal to - != = not equal to - < = less then - > = greater then	basic-4.50

Command	Description	Pack/Rel
ECNT MODL	Print the number of registered IP Phones with model name	basic-4.50
ECNT MODL <MMMM>		basic-4.50
	Print the number of registered IP Phones, where: MMMM = IP Phone model name, where: - 2001P2 = IP Phone 2001 Phase 2 - 2002 = IP Phone 2002 - 2002P2 = IP Phone 2002 Phase 2 - 2004 = IP Phone 2004 - 2004P2 = IP Phone 2004 Phase 2 - 2033 = 2033 IP Conference Phone - 2210 = IP Phone 2210 Wireless Handset	
ECNT NODE	Print registered IP Phones for all nodes	basic-4.50
ECNT NODE <nodeNum>		basic-4.50
	Print the number of registered IP Phones, where: nodeNum =the specified node	
ECNT PEC	Print the number of registered IP Phones by PEC	basic-4.50
ECNT PEC <PEC>		basic-4.50
	Print the number of IP Phones, where: PEC = Product Engineering Code	
ECNT SS	Print the number of registered IP Phones for all signaling servers	basic-4.50
ECNT SS <hostName>		basic-4.50
	Print the number of registered IP Phones, where:	

Command	Description	Pack/Rel
	hostName = host name assigned to signaling server **Note:** If the hostName variable contains an underscore (_), then an NPR001 error message is returned. An underscore is considered to be an invalid character.	
ECNT ZONE	Print the number of registered IP Phones for all zones	basic-4.50
ECNT ZONE <zoneNum> <customer>	Print the number of registered IP Phones, where: • zoneNum = specified zone • customer = customer number associated with this command	basic-4.50
ENL / DIS ERL <ERL>	Enable / Disable specified ERL.	basis-5.0
ENL / DIS L3VPN	Enable / Disable the VPN tunneling (on both sides).	basic-5.00
ENL / DIS NTP	Enable / Disable NTP. **Note:** These commands are blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer. **Note:** To apply Network Time Protocol configuration to all system elements, ensure the configuration is done using Element Manager. CLI commands only configure the Call Server, and may lead to inconsistent NTP operation at the system level.	basic-5.00
ENL / DIS RFC2833PRT	Enable / Disable the info message printing.	basic-5.00

Command	Description	Pack/Rel
ENL SHELLS SECURE	Enables all secure shells.	basic-4.50
ENL SHELLS INSECURE	Enables all unsecured shells.	basic-4.50
ENL SYSTEM RESTORE	Allow TM system restore functionality for one usage.	basic-6.00
ENL TRANSFERS INSECURE	Enable FTP (insecure File Transfer Protocol) on the system. Call server sends message through pbxLink to all connected devices and IPMG devices. **Note:** Command cannot be issued within 5 minutes of a previously issued ENL TRANSFERs or DIS TRANSFERS command.	basic-6.00
ENL TRANSFERS SECURE	Enable SFTP (secure File Transfer Protocol) on the system. Call server sends message through pbxLink to all connected devices and IPMG devices. **Important:** SFTP is required in regular operation of the CS 1000. Do not disable SFTP on VxWorks unless you have to troubleshoot a problem, if any. **Note:** Command cannot be issued within 5 minutes of a previously issued ENL TRANSFERs or DIS TRANSFERS command.	basic-6.00
EXPORT a	The EPT file stored on the hard disk (/u/db/ smpserv.db) is copied to the floppy/PC Card drive (a:/smpserv.db).	basic-4.00
EXPORT EDT	The EPT file stored on the hard disk (/u/db/ smpserv.db) is copied to the floppy/PC Card drive (a:/smpserv.db).	basic-4.00

Command	Description	Pack/Rel
EXPORT EPT	Store Event Preference Table file to disk/PCMCIA	basic-6.00
FLTH 0 - 9	Failed log in threshold (in minutes)	basic-5.00
IMPORT EPT	The EPT file stored on the floppy / PC Card (a:/smpserv.db) drive is copied to the hard drive (/u/db/smpserv.db).	basic-4.00
GEN ZONEFILE <fileName>	Generate a CSV file that contains information for all configured zones on the Call Server. You can use the <fileName> parameter to specify a file name and file path for the CSV file. If you do not specify a file name and file path, a file named zone.csv is created and stored in the /u/db directory. After you execute this command the location of the file is displayed. **Note:** The maximum length of the path/file name is 255 characters **Caution:** Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you must use bandwidth zone numbers in the range 0–255; call processing issues occur if you use bandwidth zone numbers greater than 255.	basic-7.00
IMPORT ZONEFILE <fileName>	Read a CSV file and create new zones listed in the file, or apply updates contained in the CSV file for zones that already exist. If you do not specify a file name and file path, an attempt is made to use the zone.csv file stored in the /u/db directory; otherwise the command will use the file name and file path that you specify. The output for this command is the number of zones successfully added or changed. **Note:** The maximum length of the path/file name is 255 characters **Caution:** Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you	basic-7.00

Command	Description	Pack/Rel
	must use bandwidth zone numbers in the range 0–255; call processing issues occur if you use bandwidth zone numbers greater than 255.	
INV ENTITY SETS <ON> (OFF) STATUS		basic-4.00
	Turn ON the inclusion of digital telephones and IP Phones in the Entity MIB Turn OFF the inclusion of digital telephones and IP Phones in the Entity MIB Display whether or not the digial telephones and IP Phones are included in the Entity MIB. The output displays either ON or OFF.	
INV GENERATE		
	Generate inventory CARDS, SETS, LOCRPT, ALL or ABORT	
INV GENERATE ABORT		
	Abort any currently running Inventory generations.	
INV GENERATE ALL		
	Requests for the Inventory feature to begin generating both the card and telsets Inventory file.	
INV GENERATE CARDS		
	Requests for the Inventory feature to begin generating the Inventory file for all of the cards in the system. The generation produces an inventory file with all of the cards configured on the system. Those cards that are present in the system and have card ID are noted in the inventory file with their card type, TN, and card ID. Those cards that do not have card ID or are not present in the system, is noted to be "Unavailable" in place of their card ID.	
INV GENERATE SETS		
	Requests for the Inventory feature to begin generating the Inventory file for the digital telsets with their telsets' IDs that have been configured in the system. Those telsets that are present in the system and have sets ID are noted in the inventory file with their sets type, TN, sets ID, DES, Primary DN. Those telsets that do not have sets ID or ar not present in the sytem is noted to be "Unavailable" in place of their sets ID.	
INV GENERATE ABORT		basic-5.00

Command	Description	Pack/Rel
	Abort the inventory generation for Cards, Sets and LOCRPT. System message MAT055 is printed on the TTY when Inventory Location Report is aborted.	
INV GENERATE ALL		basic-5.00
	Inventory files for Cards, Sets and LOCRPT.	
INV GENERATE LOCRPT		basic-5.00
	Inventory Location Report for all the IP Phones in the TN table. The inventory file “locrpt.inv” is generated in the path [c:]/u/db/inv/. System message MAT052 is printed on the TTY when the generation is complete.	
INV MIDNIGHT		
	Generate inventory CARDS, SETS, LOCRPT, ALL, OFF or STATUS (admin)	
INV MIDNIGHT ALL		
	Scheduling for the Midnight to run both Card and Sets Inventory generations.	
INV MIDNIGHT CARDS		
	Scheduling for the Midnight to run Card Inventory generation.	
INV MIDNIGHT OFF		
	Turns off Midnight run off Card and Sets Inventory generations.	
INV MIDNIGHT SETS		
	Scheduling for the Midnight to run Sets Inventory generation.	
INV MIDNIGHT STATUS		
	Print out the state of the Midnight schedule of Inventory.	
INV PRT	Refer to INV PRT STATUS command.	
INV PRT ALL	Requests for both the Card Inventory file and the Sets Inventory file to be printed out to the output destination (example TTY).	
INV PRT CARDS		

Command	Description	Pack/Rel
	Requests for the Card Inventory file to be printed out to the output destination (example TTY).	
INV PRT LOCRPT		basic-5.00
	Print the generated Inventory Location Report file.	
INV PRT SETS		
	Requests for the Sets Inventory file to be printed out to the output destination (example TTY)	
INV PRT STATUS		
	Requests for the status of the Inventory feature. Result may look somewhat: Inventory status: Card file status is Ok 43 records; 18/03/1999 17:10:21 Sets file status is Ok 19 records; 18/03/1999 16:44:09	
****	Abort overlay. This command can also be used to abort any Inventory file printing.	
LOCRPT ALL	Print location report for all IP phones.	basic-5.00
LOCRPT DN x		basic-5.00
	Print location report for the IP phone(s) with the specified DN (or partially-specified DN).	
LOCRPT ECL x		basic-5.00
	Print location report for the IP phone(s) in the specified ECL.	
LOCRPT ERL		basic-5.00
	Print location report for IP phones in RLM table with the specified Emergency Response Location (ERL).	
LOCRPT HWID x		basic-5.00

Command	Description	Pack/Rel
	Print location report for the IP phone with the specified (or partially-specified) Hardware Identifier (HWID)	
LOCRPT IP		basic-5.00
	Print location report for IP phones in RLM table with the specified IP Address.	
LOCRPT MANUALUPDATE/MU		basic-5.00
	Print location report for IP phones in RLM table that are Manual-Update (ManualUpdate=True).	
LOCRPT NEEDUPDATE/NU		basic-5.00
	Print location report for IP phones in RLM table that need a location update (NeedsUpdate=True).	
LOCRPT ROAMING		basic-5.00
	Print location report for the IP phone(s) that are not at home (example their Current ECL is different from their Home ECL). **Note:** This applies only when the Home ECL is not unknown (zero). This does not apply to Manual Update phones, because by definition, they are always at home.	
LOCRPT TN x		basic-5.00
	Print location report for the IP phone(s) with the specified TN (or partially-specified TN).	
LOCRPT UNALLOCATED/UNKNOWN		basic-5.00
	Print location report for IP phones in RLM table that are Auto-Update and ERL=Unknown. **Note:** This is not the same as “LOCRPT ERL 0” – ERL 0 are Auto Update phones.	
LOCRPT UNREG		basic-5.00

Command	Description	Pack/Rel
	Print location report for the IP phone(s) that are unregistered but have a TN table entry.	
`LOUT 0 - (20) - 1440`		basic-5.00
	Inactivity timeout (in minutes)	
`NEW BKPR xxx a...a b...b yy`		grprim-4.00
	Add a new Backup Rule, where: • xxx = Backup Rule number ID = (1)-100. Currently, only one rule is required for replication to the secondary system. • a...a = SCS. Currently, this is the only rule type that exists: it allows direct replication to another system. • b...b = ELAN IP address of the destination system. • yy = the number of database versions to save on the destination system = (2)-10.	
`NEW BKPR <rule number1-100> FMD [<N of versions>] [<name>]`		basic-4.50
	Change backup rule to an Fixed Media Device (FMD), where: • rule number = 1-100, Up to 100 rules can be defined. Each rule is a pattern that can be further used. FMD rules can be used by the backup schedules or for manual backup and restore operation (BKR/RSR commands activated from LD 43). • FMD = mnemonic for this rule type • N of versions = (1)-10 number of incremental backup data versions preserved on the local removable media device • name = rule name, where: text of up to 30 characters without white spaces is allowed **Note:** The <name> parameter is also added as optional when defining a new backup rule with SCS type (introduced in CS 1000 Release 4.0 Geographic Redundancy).	
`NEW BKPR <rule number> FTP <IP addr> <login><pwd> <path> [<N of versions>] [<name>]`		basic-4.50
	Change backup rule to an external FTP server, where:	

Command	Description	Pack/Rel
	• <rule number> = 1-100 Up to 100 rules can be defined. Each rule is a pattern that can be further used. These rules can be used by the Geographic Redundancy Database Replication Control (GRDRC block as defined in LD-117), by the Backup Schedules for manual backup/restore operation (BKR/RSR commands activated from Ovl.43). • FTP = mnemonic for this rule type • <IP addr> = IP address of the FTP server to be accessed for storing (Backup) or retrieving (Restore) backup data • <login> = login name to access the FTP server, up to 32 characters • <pwd> = login password to access the FTP server, up to 32 characters • <path> = path on the FTP server where the backup data file (or files for incremental versions) is located, up to 64 characters • <N of versions> = (1)-10 number of incremental backup data versions preserved on the FTP server • <name> = rule name Text of up to 30 characters without white spaces is allowed **Note:** The only backup rule type that can be referenced from GRDRC is SCS. **Note:** The <name> parameter is added as optional when defining a new backup rule with SCS type introduced in CS 1000 Release 4.0 Geographic Redundancy.	
`NEW BKPR <rule number> RMD [<N of versions>] [<name>]`	Change backup rule to a Removable Media Device (RMD), where: • <rule number> = 1-100 Up to 100 rules can be defined. Each rule is a pattern that can be further used. RMD rules can be used by the backup schedules or for manual backup and restore operation (BKR/RSR commands activated from LD 43). • RMD = mnemonic for this rule type • <N of versions> = (1)-10	basic-4.50

Command	Description	Pack/Rel
	Number of incremental backup data versions preserved on the local removable media device. • <name> = rule name Text of up to 30 characters without white spaces is allowed **Note:** The <name> parameter is also added as optional when defining a new backup rule with SCS type (introduced in CS 1000 Release 4.0 Geographic Redundancy).	
`NEW BKPS <schedule number 1-10> <Rule for BKUP> <FREQ> <DAY> <HOUR>`	Add a backup schedule, where: • <schedule number> = (1)-10 Up to 10 backup schedules can be defined. • <Rule for BKUP> = number of the backup rule for scheduled backup operation • <FREQ> = M/W/(D)/A - defines how often the scheduled backup takes place, where: - M = monthly - W = weekly - D = daily - A = automatically immediately after every EDD operation activated. There cannot be more than 1 schedule defined where FREQ = A. When <FREQ> = D, the next parameter is <HOUR> where: • <DAY> = day of the week Where: - (SU) = Sunday - MO = Monday - TU = Tuesday - WE = Wednesday - TH = Thursaday - FR = Friday - SA = Saturday - (1)- 31	basic-4.50

Command	Description	Pack/Rel
	Note: Only applicable when FREQ = W or FREQ = M. **Note:** When FREQ = M and the day specified is greater than the number of days in the current month, the backup takes place on the last day of the current month. • <HOUR> = 0-(3)-23 **Note:** This rule type is not allowed if the GRPRIM/GRSEC package is equipped and the rule is used in GRDRC.	
`NEW / OUT ELIN <erl> <tn>`	Associate / Disassociate specified TN to specified ERL. **Note:** The TN must already be configured to compose an ANI that is registered in the ALI database against this emergency location. For Small System, the TN format is “c u” For Large System, the TN format is “l s c u”.	basic-5.00
`NEW EPT aa... a INFO x`	Assign Information severity to new EPT entry, where: • aa... a = an event class with an event number (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your CHG SUPPRESS entry.	alrm_filter-21
`NEW EPT aa... a EDT x`	Assign NT-defined severity from EDT to new EPT entry, where: • aa... a = an event class with an event number (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your CHG SUPPRESS entry.	alrm_filter-21

Command	Description	Pack/Rel
NEW EPT aa... a MAJOR x	Assign Major severity to new EPT entry, where: • aa... a = an event class with an event number (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your CHG SUPPRESS entry.	alrm_filter-21
NEW EPT aa... a MINOR x	Assign Minor severity to new EPT entry, where: • aa... a = an event class with an event number (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your CHG SUPPRESS entry.	alrm_filter-21
NEW EPT aa... a CRITICAL x	Assign Critical severity to new EPT entry, where: • aa... a = an event class with an event number (e.g. BUG1000, ERR0025) • x = optional entry to escalate value of EPT entry from (0)-Suppress value, as defined by default or your CHG SUPPRESS entry.	alrm_filter-21
NEW ERL <erl> [<RT_RLI> <route_rli> <ac> <prepend> <staticELIN> <osdn>]	Add an ERL table entry, where: • <erl> = Emergency Response Location (ERL) identifier Number in the range 1-65535. • <RT_RLI> = token identifying the emergency call routing mechanism for the ERL - RT = by route number - RLI = by Route Line Index • <route_rli> = number of route or route line index (as indicated by <RT_RLI> token) - route number = as specified in LD 16	basic-5.00

Command	Description	Pack/Rel
	- route line index number = as specified in LD 86 • <ac> = access code, as specified in LD 90 • <prepend> = prepended routing digits for emergency calls • <staticELIN> = static Emergency Location Identification Number (ELIN) • <osdn> = On-Site Notification DN To skip a field and set it to blank, use either a NULL or NONE token in its place. Any fields not specified at the end of the command are set to blank, as if you entered NULL or NONE for each one.	
`NEW GRDRC xxx aaa yyy bbb ccc`	Add a GRDRC block, where: • xxx = Backup Rule number. • aaa = how the automatic database replication to the secondary system occurs (Geographic Redundancy requires that this parameter be configured as SCHD): - SCHD - according to defined backup schedule - (IMM) - immediately after any data dump operation - MIDN - after midnight data dump only - NO - not allowed • yyy = Backup Rule number used for the restore operation on the secondary system. If no rule number is entered, then this points to the <BKUP rule>. • bbb = (YES)/NO. Defines whether or not the automatic restore operation on the secondary system is allowed. • ccc = (YES)/NO. Defines whether or not the automatic sysload after successful automatic restore on the secondary system is allowed. ccc = YES is allowed only if bbb = YES.	grprim-4.00
`NEW GRSC xxx yyy zzz a..a`	Add a new GRSC block, where: • xxx = the number (N) of IP phones that must register on the secondary system for the system to escalate to the ACTIVATING state. If no value is entered, xxx = 1. The maximum value of xxx is: 10% x (Basic IP User License + IP User License). • yyy = Short Term Failure Timer, in minutes = (5) - 600	grprim-4.00

Command	Description	Pack/Rel
	• zzz = Failure Clearance Timer, in minutes = (5) - 180 • a..a = Secondary system Deactivation Mode = (AUTO)/MAN	
`NEW GRNS <FREQ><DAY><HOUR><MINUTE>[<DELAY>]`		basic-5.00
	Add a Survivable Remote Gateway Backup, where: • FREQ = defines how often the backup takes place, where: - M = monthly - W = weekly - D = daily • DAY = day of the week, applicable when FREQ = W or FREQ = M, where: - (SU) = Sunday - MO = Monday - TU = Tuesday - WE = Wednesday - TH = Thursday - FR = Friday - SA = Saturday - (1)-31 When FREQ = D, the next parameter is HOUR. • HOUR = 0-(3)-23 • MINUTE = (0)-59 • DELAY = (3)-60 The interval in minutes between two consecutively scheduled backups. The system scans for backup rules of SCS type and creates a BKPS for each of them and adjusts the start times according to the specified delayed value.	
`NEW HOST DEV_SIDE0_HSP <ip address>`		basic-4.50
	Configure the HSP ip address **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	

Command	Description	Pack/Rel
	Configure the HSP ip address **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
`NEW HOST <hostname> <IPaddress>`	Configure a new host entry, where; • host name must exist in the host table • default setting for the Primary IP address is: 137.135.128.253 • default setting for Primary Host Name is: PRIMARY_ENET • default setting for the Secondary IP address is: 137.135.128.254 • default setting for the Secondary Host Name is: SECONDARY_ENET. **Note:** Host Name Syntax: A host name can be up to 16 characters in length. The first character of a host name must be a letter of the alphabet. A character can be a letter, number, or underscore(_). A period is used as a delimiter between domain names. Spaces and tabs are not permitted. No distinction is made between upper and lower case. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
`NEW NUMZONE <numbering zone> [<site_prefix> <country_code> <npa> <ac1> <ac2> <natc> <intc> <dac> <ttbl>]`	Configure a new numbering zone with specified (optional) ZBD zone parameters. Where: • <numbering zone> = new numbering zone number A number from 1-1023. • ZBD zone parameters: - <site_prefix> = site prefix	zbd-6.00

Command	Description	Pack/Rel
	A number from 0-9999. - <country_code> = country code A number from 0-9999. - <npa> = area code (used for dialing through ZFDP) A number from 0-9999. - <ac1> = trunk access code 1 A number from 0-99. - <ac2> = trunk access code 2 A number from 0-99. - <natc> = national dial code A number from 0-9999. - <intc> = international dial code A number from 0-9999. - <dac> = flag to delete NPA for a local subscriber call A number from (0)-1. - <ttbl> = tone table A number from (0)-32. **Note:** Default values (hard-coded) are used for the ZBD numbering zone parameters, if they are not specified.	
`NEW RANGE_OF_ZONES <zoneStartNumber> <zoneAmount> <intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <zoneIntent> <zoneResourceType>`		
	Create new bandwidth zones. This command creates a range of new bandwidth zones starting from **<zoneStartNumber>**. The number of existing bandwidth zones must be less than 8001. If the number of existing bandwidth zones is greater than or equal to 8001, no bandwidth zones are created. Where: • zoneStartNumber = Zone number [0–8000] • zoneAmount = Number of zones that must be created [1-8001] • intraZoneBandwidth = Intrazone available bandwidth (0 to 0.1MBps) • intraZoneStrategy = Intrazone preferred strategy (Best Quality (BQ) or Best Bandwidth (BB)) • interZoneBandwidth = Interzone available bandwidth (0 to 0.1MBps)	basic-7.00

Command	Description	Pack/Rel
	• interZoneStrategy = Interzone preferred strategy (BQ or BB) • zoneIntent = MO (default), BMG, or VTRK • zoneResourceType = shared or private **Caution:** Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you must use bandwidth zone numbers in the range 0–255; call processing issues occur if you use bandwidth zone numbers greater than 255.	
`NEW ROUTE <network IP address> <gateway IP address>`	Configure a new routing entry <IP address>= valid IP address **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
`NEW SUBNET <IP Address> <Mask Bits> <ERL> <ECL> "<Description>"`	Add a subnet entry where: • ip address = nnn.nnn.nnn.nnn • mask = nnn.nnn.nnn.nnn • ERL and ECL = 0-65535 • Description = 20 alphanumeric characters within quotation marks.	basic-5.00
`NEW ZDID <numbering zone> <matching string> <replacement string> [<description>]`	Configure a ZBD numbering zone-based call translation table entry. Where: • <numbering zone> = 1-1023 • <matching string> = 1-16 digit “best match” numeric string Unique inside a numbering zone. • [<replacement string>] = string that replaces the matching string	zbd-6.00

Command	Description	Pack/Rel
	If <type> = SPN, CDP or ESDN, 1-16 numeric digits; if <type> = INTL, LOC, REG1, NPA, REG2 or NXX, 1-16 alphabetic characters. If <replacement string> is not specified, the matching string is deleted and not replaced. • <description> = 1-32 character textual description for the numbering zone-based call translation (ZDID) table entry If not specified, the ZDID table entry has no textual description.	
`NEW ZFDP <numbering zone> <matching string> <type> [<replacement string>] [LEN <max length>] ["<description>"]`	Create a ZBD numbering zone-based flexible dialing plan table entry. Where: • <numbering zone> = 1-1023 • <matching string> = “best match” string of 1-16 digits Unique inside a numbering zone. • <type> = values specified in the LD 15 AC1 and AC2 prompts After stripping the matching string, save the CLID type and take the following actions depending on <type> specified: - If <type> = INTL (International E.164 number), insert AC1/AC2+replacement string. - If <type> = LOC (UDP Location Code), insert AC1/AC2+ replacement string. - If <type> = REG1 (Regional Level 1), insert AC1/AC2+ZCC +replacement string. - If <type> = NPA (North American NPA), insert AC1/AC2+1, then replacement string. - If <type> = REG2 (Regional Level 2), insert AC1/AC2+ZCC +ZNPA+replacement string - If <type> = NXX (North American NXX), insert AC1/AC2+ZCC+ZNPA+replacement string - If <type> = SPN (Special Number), insert AC1/AC2+replacement string - If <type> = CDP (Coordinated Dial Plan), insert replacement string - If <type> = ESDN (Emergency Service DN), insert replacement string	zbd-6.00

Command	Description	Pack/Rel
	• [<replacement string>] = string that replaces the matching string If <type> = SPN, CDP or ESDN, 1-16 numeric digits; if <type> = INTL, LOC, REG1, NPA, REG2 or NXX, 1-16 alphabetic characters. If <replacement string> is not specified, the matching string is deleted and not replaced. • [LEN <max length>] = maximum number of dialed digits expected to match If not specified, default is to match digits for all multiple matches. • [<description>] = textual description of the numbering zone-based flexible dialing plan (ZFDP) table entry If not specified, the ZFDP table entry has no textual description.	
`NEW ZONE xxxx p1 p2 p3 p4 <shared/private>`		
	Create a new zone with the following parameters: • xxx = 0–255 zone number • xxxxx = 0–8000 zone number	basic-7.00
	• xxx = 0–255 zone number • xxxxx = 0–8000 zone number • p1 = intrazone available bandwidth 0-100000 kbits/s • p2 = intrazone preferred strategy, where: - (BQ for Best Quality - BB for Best Bandwidth) • p3 = interzone available bandwidth 0-100000 kbits/s • p4 = intrazone preferred strategy - (BQ for Best Quality - BB for Best Bandwidth) • (Shared) = ethersets configured in shared zones use DSP resources configured in shared zones. If all of the shared zones' gateway channels are used, the caller receives an overflow tone and the call is blocked. The order of channel selection for the gateway channels is: - channel from same zone as etherset is configured - any available channel from the shared zones' channels • Private = new zone type introduced by IPL 3.0. DSP channels configured in a private zone are used only by ethersets which	basic-4.50 basic-7.00

Command	Description	Pack/Rel
	have also been configured for that private zone. If more DSP resources are required by these ethersets than are available in the zone, DSPs from other zones is used. However, ethersets configured in shared zones cannot use the private zones' channels. The order of selection for the gateway channels is: - channel from same private zone as etherset is configured - any available channel from the pool of shared zones' channels **Caution:** Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you must use bandwidth zone numbers in the range 0–255; call processing issues occur if you use bandwidth zone numbers greater than 255.	
`NEW ZONE <x...x>`	Create a new Zone with the following default bandwidth values: • 10KBps for Intrazone available bandwidth • BQ for iIntrazone preferred strategy • 10KBps for Interzone available • BQ for Interzone preferred strategy	
`NEW ZONE <x...x> aa`	Create a new Zone, where: aa = one of the following bandwidths: - p1 = Intrazone available bandwidth (0 to 0.1MBps) - p2 = Intrazone preferred strategy (BQ for Best Quality or BB for best Bandwidth) - p3 = Interzone available bandwidth (0 to 0.1MBps) - p4 = Interzone perferred strategy (BQ or BB)	
`NEW ZONE <zoneNumber> [<intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <zoneIntent> <zoneResourceType>]`	Configure a new zone, where:	zcac-4.50

Command	Description	Pack/Rel
	• zoneNumber = 0–255 • Zone = 0–8000 • intraZoneBandwidth = 0-.1Mbps • intraZoneStrategy = intrazone preferred strategy, where: - BQ = Best Quality - BB = Best Bandwidth • interZoneBandwidth = 0-.1Mbps • interZoneStrategy = interzone preferred strategy, where: - BQ = Best Quality - BB = Best Bandwidth • zoneIntent = type of zone, where: - MO = Main Office zone - BMG = Branch Media Gateway zone - VTRK = Virtual Trunk zone • zoneResourceType = resource Intrazone preferred strategy, where: - (shared) = shared DSP channels - private = private DSP channels **Caution:** Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you must use bandwidth zone numbers in the range 0–255; call processing issues occur if you use bandwidth zone numbers greater than 255.	zcac-7.00
`OUT BKPR <rule number>`	Remove backup rule, where <rule number> = a rule number from 1-100. If no rule number is entered, then all backup rules are removed.	grprim-4.00
`OUT BKPS <schedule number 1-10>`	Remove backup schedule	basic-4.50
`OUT EPT <a...a> | ALL`		alrm_filter-21

Command	Description	Pack/Rel
	Delete an entry in the Event Preference Table (EPT) Where: • a...a = identifier of EPT table entry • ALL = delete all EPT table entries	
OUT ERL <ERL#>	Delete an ERL entry.	
OUT GRDRC	Remove current GRDRC Block	grprim-4.00
OUT GRNS	Remove all backup schedules that reference backup rules of type SCS.	basic-5.00
OUT GRSC	Remove GRSC Block	grprim-4.00
OUT HOST nnn	Delete configured host entry (delete host from network host table). **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
OUT HSP_MASK	Removes the configured HSP subnet mask from the Call Server and replaces it with the default HSP subnet mask **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	basic-4.50
OUT RANGE_OF_ZONES	Remove a range of existing bandwidth zones. This command deletes a range of existing bandwidth zones, starting from <zoneStartNumber>. If there are no bandwidth zones with a zone number greater than <zoneStartNumber>, then no bandwidth zones are deleted.	basic-7.00

Command	Description	Pack/Rel
	Where: • zoneStartNumber = Zone number [0–8000] • zoneAmount = Number of zones that must be deleted [1-8001]	
`OUT NUMZONE <numbering zone)`		zbd-6.00
	Remove a ZBD numbering zone, where <numbering zone) = a number from 1-1023.	
`OUT ROUTE nn`		
	Delete configured routing entry	
`OUT SUBNET <IP Address> <Mask Bits>`		basic-5.00
`OUT ZDID <numbering zone> <matching string>`		zbd-6.00
	Delete a ZBD numbering zone-based call translation. Where: • <numbering zone> = 1-1023 • <matching string> = “best match” string of 1-16 digits Unique inside a numbering zone.	
`OUT ZFDP <numbering zone> <matching string>`		zbd-6.00
	Delete a ZBD numbering zone-based flexible dialing plan. Where: • <numbering zone> = 1-1023 • <matching string> = “best match” string of 1-16 digits Unique inside a numbering zone.	
`OUT ZONE <x...x>`		
	Remove an existing zone.	
`PDT (NO)/ PDT1 / PDT2`		basic-5.00
	PDT Access. **Note:** Aavailable only when adding/modifying LAPW, Level 1 (PWD1) and Level 2 (PWD2) users.	
`PORT ACCESS CUSTOM`		basic-6.00

Command	Description	Pack/Rel
	Configures a custom Access Restrictions ruleset defining port access rules for the system. Issuing this command results in the following actions by the system: 1. Check to ensure a custom Access Restrictions rules file exists in the appropriate directory structure. If not, an error is displayed and the command aborted. 2. Displays a warning that enabling a custom Access Restrictions rules file could possibly have detrimental effects on the system, and prompts the user to confirm the action (Y or N). 3. Check to ensure that the custom Access Restrictions rules file will load. If not, an error is displayed and the command aborted. 4. If the VxWorks firewall state indicates that the Access Restrictions feature is already enabled, disable the existing Access Restrictions rules, including mandatory Access Restrictions rules. 5. If the VxWorks firewall state indicates that the Access Restrictions feature is not already enabled, enable it and set the default Access Restrictions rule to ACCEPT ALL. Any old Access Restrictions statistics are cleared. 6. Load the mandatory Access Restrictions rules file. 7. Load the custom Access Restrictions rules file. If a problem is encountered when loading the custom Access Restrictions rules file, the system displays an error, aborts the command, and returns the Access Restrictions feature to its previous state. 8. Change the VxWorks firewall state on the Call Server to Custom. An information message is logged on the Call Server indicating that the Access Restrictions feature is operating with a custom Access Restrictions rules file. 9. Send a VxWorks firewall state change message to all endpoints with the mandatory and custom Access Restrictions rules files version numbers. An information message is logged on each endpoint indicating that the Access Restrictions feature is operating with a custom Access Restrictions rules file. **Note:** When a PORT ACCESS command (CUSTOM, DEFAULT, OFF) is entered, all other PORT ACCESS commands are suspended for a pre-determined or incremental amount of time depending on the number of endpoints, to allow	

Command	Description	Pack/Rel
	sufficient time to propagate the state change to all endpoints.	
PORT ACCESS DEFAULT		basic-6.00
	Configures the default Access Restrictions ruleset defining port access rules for the system. Issuing this command results in the following actions by the system: 1. Check to ensure a default Access Restrictions rules file exists in the appropriate directory structure. It is not expected that any errors will occur when processing the default Access Restrictions rules file. 2. If the VxWorks firewall state indicates that the Access Restrictions feature is already enabled, delete the existing Access Restrictions rules, including mandatory Access Restrictions rules. 3. If the VxWorks firewall state indicates that the Access Restrictions feature is not already enabled, enables it and sets the default Access Restrictions rule to ACCEPT ALL. Any old Access Restrictions statistics are cleared. 4. Load the mandatory Access Restrictions rules file. 5. Load the default Access Restrictions rules file. 6. Change the VxWorks firewall state on the Call Server to Default. An information message is logged on the Call Server indicating that the Access Restrictions feature is operating with a default Access Restrictions rules file. 7. Send a VxWorks firewall state change message to all endpoints with the default and custom Access Restrictions rules files versions as zeros. An information message is logged on each endpoint indicating that the Access Restrictions feature is operating with a default Access Restrictions rules file. **Note:** When a PORT ACCESS command (CUSTOM, DEFAULT, OFF) is entered, all other PORT ACCESS commands are suspended for a pre-determined or incremental amount of time depending on the number of endpoints, to allow sufficient time to propagate the state change to all endpoints.	
PORT ACCESS OFF		basic-6.00

Command	Description	Pack/Rel
	Disables all Access Restrictions rules in the system. Issuing this command results in the following actions by the system: 1. Disable all enabled Access Restrictions rules. 2. Deactivate the VxWorks firewall facility. 3. Change the VxWorks firewall state on the Call Server to OFF. An information message is logged on the Call Server indicating that the Access Restrictions feature is not operational. 4. Send a VxWorks firewall state change message to all endpoints with the default and custom Access Restrictions rules files versions as zeros. An information message is logged on each endpoint indicating that the Access Restrictions feature is not operational. **Note:** When a PORT ACCESS command (CUSTOM, DEFAULT, OFF) is entered, all other PORT ACCESS commands are suspended for a pre-determined or incremental amount of time depending on the number of endpoints, to allow sufficient time to propagate the state change to all endpoints.	
`PORT ACCESS SHOW CUSTOM`		basic-6.00
	Display the Access Restrictions rules in the CUSTOM Access Restrictions rules file in tabular format.	
`PORT ACCESS SHOW DEFAULT`		basic-6.00
	Display the Access Restrictions rules in the DEFAULT Access Restrictions rules file in tabular format.	
`PORT ACCESS STATUS [ALL]`		basic-6.00
	Display the global state of the Access Restrictions feature. If the [ALL] parameter is specified, the system polls all endpoints to determine their local Access Restrictions state: • If there are any cards that don't have matching file signatures, or that can't be contacted, they are displayed. A list of the possible failures is as follows: - CS local state incorrect: <CS state>	

Command	Description	Pack/Rel
	- <endpoint IP> <endpoint type> state not received - <endpoint IP> <endpoint type> has incorrect state of <bad state> - <endpoint IP> <endpoint type> has incorrect default and custom file - <endpoint IP> <endpoint type> has incorrect default file - <endpoint IP> <endpoint type> has incorrect custom file • If all cards have matching file signatures, a message is displayed indicating that all endpoints match.	
PORT ACCESS VALIDATE		basic-6.00
	Validates the rules in a CUSTOM file and Prints out what is wrong with the file.	
PRT ADMIN_COMM		basic-4.00
	Print the administration group read-only community name strings.	
	If administration group community strings have been added or modified in LD117 since the last execution of the SYNC SNMPCONF command, the PRT ADMIN_COMM command prints the added and modified strings in an "OVLY 117 Configuration" area and the existing community strings in an "ACTIVE Configuration" area. When the SYNC SNMPCONF command is executed, the "OVLY 117 Configuration" changes are activated and become part of the "ACTIVE Configuration" on the system.	basic-6.00
PRT APPSRV		
	Print the IP address of the application server for PD.	
PRT AQOS <attribute> <zone / ALL>		basic-4.5
	Prints QoS records for specified attribute and zone (or for all zones with ALL). Where: Attribute = 1 - 32 Defined in the Traffic Report 16 (see *Avaya Traffic Measurement Formats and Outputs Reference, NN43001-750*), for example "Interzone warning jitter count".	
PRT BKPR xxx		grprim-4.00

Command	Description	Pack/Rel
	Print backup rule, where: xxx = a rule number ID 1-100 If no rule number is entered, then all backup rules are printed.	
`PRT BKPR <rule number 1-100>`		basic-4.50
	Print backup rule, where: rule number = 1-100	
`PRT BKPS ALL`		basic-4.50
	Print all backup schedules	
`PRT BKPS <schedule number 1-10>`		basic-4.50
	Print backup schedule	
`PRT CAB`		
	Prints all data related to survivability.	
`PRT DNIP <DN> [<CustomerNo>]`		
	Pint a list of IP addresses for each IP Phone registered with the specified DN. **Note:** A partial DN can be entered. Sample output: => PRT DNIP 4000 0 (only search customer 0 for DN) CUST 00 DN 4000 TN Type Key IP Address Zone Status ---------- 061-01 i2002 03 SCR 47.11.215.41 000 REG 061-00 i2004 00 SCR 47.11.215.39 000 REG => prt dnip 4000 (same DN in different customers) CUST 00 DN 4000 TN Type Key IP Address Zone Status ---------- 061-01 i2002 03 SCR 47.11.215.41 000 REG 061-00 i2004 00 SCR 47.11.215.39 000 REG CUST 01 DN 4000 TN Type Key IP Address Zone Status ---------- 061-10 i2004 05 MCR 47.11.215.38 001 REG	
`PRT EDT aa... a`		alrm_filter-21
	Print a single Event Default Table (EDT) event, where:	

Command	Description	Pack/Rel
	aa... a = an event class with an event number (e.g. BUG1000, ERR0025)	
`PRT EDT aa... a bb...b`		alrm_filter-21
	Print a range of Event Default Table (EDT) events, where: • aa... a = first entry in EDT event range (e.g. BUG1000, ERR0025) • bb...b = last entry in EDT event range (e.g. BUG1000, ERR0025)	
`PRT EDT <severity <eventID> <eventID>`		basic-4.00
	The entries in the EDT can be listed based on the severity field for all entries or the specified range of entries.	
`PRT ELIN [ALL] / <erl>`		basic-5.00
	Print ELINs for ALL / specified ERL.	
`PRT ENABLE_TRAPS`		basic-6.00
	Display the enabled/disabled parameter for all SNMP traps.	
`PRT ELNK`	Display active and inactive Ethernet interface IP addresses (display active and inactive ELAN IP addresses). **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
`PRT EPT aa... a`		alrm_filter-21
	Print a single Event Preference Table (EPT) entry, where: aa... a = an event class with an event number (e.g. BUG1000, ERR0025	
`PRT EPT aa... a bb...b`		alrm_filter-21
	Print specific Event Preference Table (EPT) entry, where:	

Command	Description	Pack/Rel
	• aa... a = first entry in EPT event range (e.g. BUG1000, ERR0025) • bb...b = last entry in EPT event range (e.g. BUG1000, ERR0025)	
PRT EPT ALL	Print all entries in Event Preference Table (EPT)	alrm_filter-21
PRTS PRTS EDT		basic-4.00
	Print entries in Event Default Table by Severity	
PRTS EPT severity <eventID> <eventID>		basic-4.00
	The entries in the EPT can be listed based on the severity field for all entries or the specified range of entries.	
PRT ERL [ALL]		basic-5.00
	Print all ERL entries.	
PRT ERL [<ERL #> [<+/-Count>]		
	Print the specified ERL entry, or a “page” of ERLs starting from the specified ERL..	
PRT ES1	Print Echo Server 1's IP address and port number.	basic-4.00
PRT ES2	Print the Echo Server 2's IP address and port number.	basic-4.00
PRT ESS	Print both Echo Server's IP address and port number.	basic-4.00
PRT FMT_OUTPUT		alrm_filter-21
	Print formatted output string	
PRT GRDRC	Print GRDRC Block	grprim-4.00
PRT GRSC	Print GRSC Block	grprim-4.00

Command	Description	Pack/Rel
PRT HOST	Display network host table entries (enabled and disabled hosts). **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
PRT HSP_MASK	Retrieves the manually configured HSP mask from the Call Server if it exists and outputs it to the screen, otherwise it prints the default HSP subnet mask (255.255.255.0) **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
PRT INTERZONE {<nearZone>} {<farZone>} {<nearVPNI>} {<farVPNI>}	Print interzone statistics between near (VPNI - Zone) and far (VPNI - Zone), where: • NEAR END = ZONE and VPNI • FAR END = ZONE and VPNI • State = ENL/DIS • Type= PRIVATE/SHARED • Strategy = BB/BQ • ZoneIntent = MO/BMG/VTRK • QoS factor = % • Bandwidth = number of Kbps • Sliding Max = number of Kbps • Usage = number of Kbps • Peak = % • Average = number of Kbps • Alarms = Aph **Note:** The report rows are grouped as:	zcac-4.50

Command	Description	Pack/Rel
	• First row = summary bandwidth usage per near zone • Next rows = bandwidth usage per near (VPNI- Zone) and far (VPNI - Zone) • With release 4.50 the PRT ZONE command is not used. **Note:** The interzone command printout shows the Bandwidth usage for inter zone calls only.	
`PRT INTRAZONE {<zone>}`		zcac-4.50
	Print intrazone statistics for all or for the identified zone, where: • Zone = 0–255 • Zone = 0–8000 • State = ENL/DIS • Type = PRIVATE/SHARED • Strategy = BB/BQ • ZoneIntent = MO/BMG/VTRK • Bandwidth = number of Kbps • Usage = number of Kbps • Peak = % **Note:** The intrazone command printout shows bandwidth usage for both intra and inter zone calls.	zcac-7.00
`PRT IPDN <IPAddress>`		

	Print a list of DNs configured for the specified IP address.
	
	Sample output for PRT IPDN 47.11.215.38:
	
	`IP 47.11.215.38`
	`CUST 01 TN 061-10 TYPE i2004 ZONE 001 REG`
	`Key DN CPND Name`
	`---------------------------------------------`
	`00 SCR 4010 I2004_1 VLN61-10`
	`05 MCR 4000 i2004_cust1 vln61_10`
	
	Note:
	An IP address can be specified with only the leading digits (for example, 47.11). An IP address with zeroes at the end can be specified (for example, 47.11.0.0)	

Command	Description	Pack/Rel
PRT IPR x	Prints the IP connectivity configuration data associated with the IP Expansion cabinet end of the specified port, where x = 1-4. supl shelf IPMG supl shelf or <CR> to print information for all IPMGs. If an IPMG supl shelf is not entered, all IPMGs are output, without their designator information. If an IPMG supl shelf is entered, a single IPMG is output, with the designator information (if MGC based IPMG)	
PRT IPM x	Prints the IP connectivity configuration data associated with the Main cabinet end of the specified port, where: x = 1-4	
PRT IPMG	supl shelf IPMG supl shelf or <CR> to print information for all IPMGs. If an IPMG supl shelf is not entered, all IPMGs are output, without their designator information. If an IPMG supl shelf is entered, a single IPMG is output, with the designator information (if MGC based IPMG)	
PRT LCL Prints the Local Core Location Loop, Shelf & Card values (Applicable only to CP PM and Linux CS)		basic-6.00
PRT L3ELAN [side / CR] [role / CR] Display the physical addresses of the CS cores. Where: • Side = 0 / 1 (number of the core) • Role = ACTIVE / INACTIVE.		basic-5.00
PRT L3GW [side] Display the default gateway for physical ELAN. Where: Side = 0 / 1 (number of the core)		basic-5.00
PRT L3HSP <side / CR> Display Layer 3 Hot Standby Protocol of VPN Router Where: Side = 0 / 1 (number of the core)		basic-5.00
PRT L3HSPGW [side / CR]		basic-5.00

Command	Description	Pack/Rel
	Display Layer 3 Hot Standby Gateway of VPN Router Where: Side = 0 / 1 (number of the core)	
`PRT L3HSPMASK [side / CR]`		basic-5.00
	Display Layer 3 Hot Standby Mask of VPN Router Where: Side = 0 / 1 (number of the core)	
`PRT L3MASK [side / CR]`		basic-5.00
	Display the ELAN mask. Where: Side = 0 / 1 (number of the core)	
`PRT L3PRIV [role]`		basic-5.00
	Display the ELAN virtual ACTIVE and INACTIVE addresses. Where: • Side = 0 / 1 (number of the core) • Role = ACTIVE / INACTIVE.	
`PRT LDAPSYNC`		basic-6.00
	Display the parameters of the Unicode Name Directory <-> CND LDAP scheduled data synchronization task.	
`PRT MASK`		basic-5.00
	Display subnet mask stored in database. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
`PRT MEDS`		
	Print Mediation Server Selection feature	
`PRT MGMT_ALARM`		
	Print MGMT SNMP traps setting	

Command	Description	Pack/Rel
PRT MSEC ALL		basic-5.00
	Print System-wide media security configuration, and the media security CLS for all TNs.	
PRT MSEC IP <ip_addr>		basic-5.00
	Print Media SECcurity class of service (CLS) for a specified IP address where: <ip_addr> = full or partial IP address	
PRT MSEC SYS		basic-5.00
	Print system wide Media SECurity configuration.	
PRT MSEC TN		basic-5.00
	Print Media SECurity CLS for a specified full or partial TN.	
PRT NAV_SITE		basic-4.00
	Print the navigation site name	
	If the navigation site name has been modified in LD117 since the last execution of the SYNC SNMPCONF command (not activated), the PRT NAV_SITE command prints the modified navigation site name in an "OVLY 117 Configuration" area and the existing navigation site name in an "ACTIVE Configuration" area. When the SYNC SNMPCONF command is executed, the "OVLY 117 Configuration" changes are activated and become part of the "ACTIVE Configuration" on the system.	basic-6.00
PRT NAV_SYSTEM		basic-4.00
	Print the navigation system name	
	If the navigation system name has been modified in LD117 since the last execution of the SYNC SNMPCONF command (not activated), the PRT NAV_SYSTEM command prints the modified navigation system name in an "OVLY 117 Configuration" area and the existing navigation system name in an "ACTIVE Configuration" area. When the SYNC SNMPCONF command is executed, the "OVLY 117 Configuration" change is activated and becomes part of the "ACTIVE Configuration" on the system.	basic-6.00

Command	Description	Pack/Rel
PRT NBWMM CFG	Print CS Configuration table	
PRT NBWMM REG	Print CS Registration Information table	
PRT NBWMM STAT	Print CS Network status table	
PRT NDAPP	Print the Name Directory application parameters. => PRT NDAPP NDApplState=Enabled NDlookupTimer=4000	basic-6.00
PRT NKT	Print NAT Mapping Keep Alive time-out setting of port mapping for devices behind a NAT router.	basic-4.00
PRT NTP	Display the current configuration parameters of NTP. Displayed parameters include: • IP addresses of primary and secondary NTP servers • values for the three threshold levels: Minimum, Warning, and Maximum • security mode: secure or insecure • Key ID (if NTP is running in secure mode) • time interval • local time zone offset from UTC • synchronization mode: manual or background **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	basic-5.00
PRT NUMZONE <numbering zone)		zbd-6.00

Command	Description	Pack/Rel
	Print a table of information for a ZBD numbering zone, where <numbering zone> = 1-1023. Output: • <PREF> = site prefix A number from 0-9999. • <CC> = country code A number from 0-9999. • <NPA> = area code (used for dialing through ZFDP) A number from 0-9999. • <AC1> = trunk access code 1 A number from 0-99. • <AC2> = trunk access code 2 A number from 0-99. • <NATC> = national dial code A number from 0-9999. • <INTC> = international dial code A number from 0-9999. • <DAC> = flag to delete NPA for a local subscriber call A number from (0)-1. • <TTBL> = tone table A number from (0)-32. **Note:** If <numbering zone> is not specified, all numbering zones are printed.	
PRT NZDES [<numbering zone>]		zbd-6.00
	Print the description for a specified ZBD numbering zone. **Note:** Descriptions for all numbering zones are printed if <numbering zone> is not specified.	
PRT OPEN_ALARM		
	Display SNMP open alarm trap settings.	
	If SNMP open alarm trap settings have been added or modifed in LD117 since the last execution of the SYNC SNMPCONF command, the PRT OPEN_ALARM command displays the new (not yet activated) SNMP open alarm trap settings in an "OVLY 117 Configuration" area, and the existing (currently active) SNMP open alarm trap settings in an "ACTIVE Configuration" area. When the SYNC SNMPCONF command is executed, the	basic-6.00

Command	Description	Pack/Rel
	"OVLY 117 Configuration" open alarm changes are activated and become part of the "ACTIVE Configuration" on the system.	
PRT PDBAK	Print parameters for remote backup of PD	
PRT PDV	Print the current PDV value	
PRT PPP	Print Point-to-point Protocol interface address(es)	
PRT PTM	Print current Point-to-point Protocol idle timer settings	
PRT QOS	Print the current and average QOS values	
PRT QSTHS	Print all VQ thresholds	pvqm-4.0
PRT RCL	Prints the Remote Core Location Loop, Shelf & Card values (Applicable only to CP PM and Linux CS).	
PRT ROUTE	Display routing table entries stored in the database. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
PRT SEL [nn] [aaaa]	Print most recent record(s) in system event list, where: • [nn] = 0-(20)-SELSIZE • [aaaa] = category name (for example, BUG) All categories are printed if not specified.	basic-4.5
PRT SELSIZE	Print System Event List size	
PRT SNMP_SYSGRP	Print all parameters of the MIB-II system group.	basic-4.00
	If MIB-II system group parameters have been modified in LD117 since the last execution of the SYNC SNMPCONF command (not activated), the PRT SNMP_SYSGRP command prints the modified MIB-II system group parameters in an "OVLY 117 Configuration" area and the existing MIB-II system group	basic-6.00

Command	Description	Pack/Rel
	parameters in an "ACTIVE Configuration" area. When the SYNC SNMPCONF command is executed, the "OVLY 117 Configuration" changes are activated and become part of the "ACTIVE Configuration" on the system.	
PRT SUBNET [ALL]		basic-5.00
	Print all subnet entries.	
PRT SUBNET ECL <ecl>		basic-5.00
	Print all subnets that match the specified ECL.	
PRT SUBNET ERL<erl>		basic-5.00
	Print all subnets that match the specified ERL.	
PRT SUBNET <IP Address>		basic-5.00
	Print the specified subnet entry (or all entries that match a partially-specified IP address).	
PRT SUBNET NTH <n-th> <count>		basic-5.00
	Print ‘count’ subnets starting from ‘n-th’ entry.	
PRT SUPPRESS		alrm_filter-21
	Print global suppress value	
PRT SUPPRESS_ALARM		basic-4.00
	Prints the alarm suppression threshold value.	
PRT SYSMGMT_COMM		basic-4.00
	Print the system management Read/Write/Trap community name strings	
	If system management read/write/trap community strings have been added or modified in LD117 since the last execution of the SYNC SNMPCONF command (not activated), the PRT SYSMGMT_COMM command prints the added and modified system management read/write/trap community strings in an	basic-6.00

Command	Description	Pack/Rel
	"OVLY 117 Configuration" area and the existing system management read/write/trap community strings in an "ACTIVE Configuration" area. When the SYNC SNMPCONF command is executed, the "OVLY 117 Configuration" changes are activated and become part of the "ACTIVE Configuration" on the system.	
PRT TIMER	Print global timer window length (in minutes). See Global window timer length on page 364for more information.	alrm_filter-21
PRT VPNKEY		basic-5.00
	Display the pre-shared key:	
PRT VPNNET		basic-5.00
	Display both VPN Network IP and Mask	
PRT VPNROUTER <side / CR> <address type / CR>		basic-5.00
	Display interface of VPN Router Where: • Side = 0 / 1 (number of the core) • Address type = ‘PUBLIC’ / ‘PRIVATE’ VPN Router interface	
PRT ZACB [<Zone>]		
	Print branch office zone dialing plans, where <zone> = branch office zone. If <zone> is not specified, print branch office zone dialing plans for all branch office zones.	
PRT ZALT [<zone number>]		basic-4.50
	Print Alternative Prefix numbers, where <zone number> = 0–255. Print Alternative Prefix numbers, where <zone number> = 0–8000. If <zone number> is not specified, print Alternate Prefix numbers for all configured zones.	basic-7.00
PRT ZAST	Print Alarms Suppress time interval for the zone.	
PRT ZBW [<Zone>]		
	Print zone bandwidth utilization, where <zone> = zone.	

Command	Description	Pack/Rel
	If <zone> is not specified, print zone bandwidth utilization for all configured zones.	
PRT ZBWM <Source Zone> [<Dest Zone>]		basic-4.50
	Print a zone-to-zone QoS status for all zones, where:	
	• Source Zone = 0–255	basic-7.00
	• Source Zone = 0–8000	basic-7.00
	• Dest Zone = 0–255	
	• Dest Zone = 0–8000	
PRT ZBWM <Source Zone> ALL		basic-4.50
	Print a zone-to-zone QoS status table for all zones, where,	
	• Source Zone = 1-255	basic-7.00
	• Source Zone = 1-8000	
	Table Output Fields are:	
	• Source — Zone and VPNI	
	• Destination — Zone and VPNI	
	• QoS factor	
	• Configured Interzone B/W (Kbps)	
	• Sliding Maximum B/W (Kbps)	
	• Actual instantaneous B/W used (Kbps)	
	• Calls/hour or average bandwidth (Kbps)	
PRT ZBWM <Source Zone> [<Destination Zone>]		
	Print a zone-to-zone QoS status table, where:	
	• Source Zone = 0–255	basic-7.00
	• Source Zone = 0–8000	basic-7.00
	• Destination Zone = 0–255, and	
	• Destination Zone = 0–8000	
	Output Fields are:	
	• Source — Zone and VPNI	
	• Destination — Zone and VPNI	
	• QoS factor	

Command	Description	Pack/Rel
	• Configured Interzone B/W (Kbps) • Sliding Maximum B/W (Kbps) • Actual instantaneous B/W used (Kbps) • Calls/hour or average bandwidth (Kbps)	
`PRT ZCAC {<zone>}`		zcac-4.50
	Print CAC parameters for all or for the identified zone, where: • Local Zone = 0–255 • Local Zone = 0–8000 • State = ENL/DIS • CR =1-100 • CPL =1-100 • CD =1-100 • CJ = 1-100 • CQOS = 1-100 • ZQRT = 1-100 • ZQRTI = 10-120 • ZQUAT = 1-99 • ZQWAT =1-99 • CACVT = 1-255	zcac-7.00
`PRT ZDES [<DESMatchString>]`		
	Print a table of the zone description entries.	
`PRT ZDID [<numbering zone>] [<matching string>]`		zbd-6.00
	Print a table of ZBD numbering zone-based call translations. Where: • <numbering zone> = 1-1023 • <matching string> = “best match” string of 1-16 digits Unique inside a numbering zone. Only numbering zone-based call translations with the specified 1-16 digit numeric matching string are printed If not specified, all numbering zone-based call translations are printed.	
`PRT ZDP [<Zone>]`		

Command	Description	Pack/Rel
	Print a table of branch office zone dialing plan entries.	
`PRT ZESA [<Zone>]`		
	Print a table of branch office zone EmergencyServices Access (ESA) entries.	
`PRT ZDST`		
	Print a table of branch office zone time adjustment properties entries.	
`PRT ZFDP [<numbering zone>] [<matching string>]`		basic-6.00
	Print a table of ZBD numbering zone-based flexible dialing plans. Feature 420 (Zone Based Dialing) must be equipped. Where: • <numbering zone> = 1-1023 If not specified, all numbering zone-based flexible dialing plans are printed. • <matching string> = 1-16 digit numeric string Unique inside a numbering zone. Only numbering zone-based flexible dialing plans with the specified 1-16 digit matching string are printed. If not specified, all numbering zone-based flexible dialing plans are printed.	
`PRT ZONE ALL`		
	Print zone information for all configured zones	
`PRT ZONE <x...x>`		
	Print zone information for a specific zone, where: • ZoneNumber = 0–255 • ZoneNumber = 0–8000	pvqm-7.00
`PRT ZPAGE`		
	This commands prints zone information for <zonesPerPage> zones starting from zone number <zoneNumber>. Data is printed for the following categories: • zone number • intrazone bandwidth • intrazone strategy	

Command	Description	Pack/Rel
	• interzone bandwidth • interzone strategy • resource type • zone intent • description	
PRT ZPARM [<numbering zone>]	Print the parameters of a ZBD numbering zone, where <numbering zone> = 1-1023. **Note:** When no numbering zone is specified, parameters for all ZBD numbering zones are printed.	zbd-6.00
PRT ZQNL <ZoneNumber>	Print the Notification Level for the specified zone, where: • ZoneNumber = 0–255 • ZoneNumber = 0–8000	pvqm-4.0 pvqm-7.00
PRT ZQNL ALL	Print the Notification Level for all zones.	pvqm-40
PRT ZQOS <zone> <attribute / ALL>	Prints QoS records for specified attribute and zone (or for all attributes with ALL). Where attribute is defined in the Traffic Report 16 (see *Avaya Traffic Measurement: Formats and Outputs Reference, NN43001-750*), for example "Interzone warning jitter count".	basic-4.5
PRT ZTDF [<Zone>]	Print a table of branch office zone time adjustment properties entries	
PRT ZTP [<Zone>]	Print a table of branch office zone time adjustment properties entries.	
REGISTER UCMSECURITY CS		

Command	Description	Pack/Rel
	Establish mutual trust with the Primary Security Server for the Call Server. If the Call Server is already registered, it re-registers.	
REGISTER UCMSECURITY DEVICE		
	Establish mutual trust with the Primary Security Server for the element.	
REGISTER UCMSECURITY SYSTEM		
	Establish mutual trust with the Primary Security Server for only the Call Server and any unregistered elements. It will not re-register elements that are already registered.	
REGISTER UCMSECURITY SYSTEM FORCE		
	Establish mutual trust with the Primary Security Server for all system elements regardless if they are already registered.	
RELOAD EPT		basic-4.00
	The new/modified EPT file is loaded into memory from disk (/u/db/smpserv.db).	
RST DN	Reset IP sets with specified DN	
RST ELNK ACTIVE		
	Reset Meridian 1 active Ethernet interface IP address to default value (reset active ELAN IP address to default). **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
RST ELNK INACTIVE		
	Reset Meridian 1 inactive Ethernet interface IP address to default value (reset inactive ELAN IP address to default). **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	

Command	Description	Pack/Rel
RST FW	Print all scheduled reset times	basic-4.50
RST FW <FWID>	Print all scheduled reset times by firmware ID	basic-4.50
RST FW <FWID> START	Immedicate hard-reset all IP Phones, where: FWID = firmware ID of IP Phones	basic-4.50
RST FW <FWID> <START/STOP> <HH:MM>	Schedule or cancel hard-reset all IP Phones, where: • FWID = firmware ID of IP Phones • START/STOP = IP Phones reset, where: - START = set reset time schedule - STOP = cancel scheduled reset • HH:MM = hour and minute when IP Phones are reset	basic-4.50
RST IPR x	Restores the default IP connectivity configuration for the IP Expansion cabinet end of the specified port, where: x = 1-4	
RST IPM x	Restores the default IP connectivity configuration for the Main cabinet end of the specified port, where: x = 1-4	
RST MASK	Reset subnet mask to default	
RST PPP LOCAL	Reset local Point-to-point Protocol interface IP address to default value	
RST PPP REMOTE	Reset remote Point-to-point Protocol interface IP address to default value	

Command	Description	Pack/Rel
RST PTM	Reset Point-to-point Protocol idle timer to default	
RST TN	Reset IP set with specified TN	
RST ZONE	Print all scheduled reset times	basic-4.50
RST ZONE <ZoneNumber>	Print all scheduled reset times by zone	basic-4.50
RST ZONE <ZoneNumber> START	Hard-reset all IP Phones, where: ZoneNumer = zone number	basic-4.50
RST ZONE <ZoneNumber> <START/STOP> <HH:MM>	Schedule or cancel hard-reset all IP Phones, where: • ZoneNumer = zone number • START/STOP = IP Phones reset, where: - START = set reset time schedule - STOP = cancel scheduled reset • HH:MM = hour and minute when IP Phones are reset	basic-4.50
SECRET DEFAULT	Set the Secret to default value.	
SECRET SET	Define the Secret	
SECRET STAT	Print the Secret	
SECURITY DOMAIN JOIN	Establish mutual trust with the UCM Primary Security Server.	basic-6.00

Command	Description	Pack/Rel
SECURITY DOMAIN LEAVE	Remove the UCM Primary Security Server mutual trust information from the device.	basic-6.00
SECURITY DOMAIN MODE [MANUAL | USER | AUTO]	Configure the UCM security domain management mode on the Call Server. Where: • MANUAL = all devices must join the UCM security domain using local CLI commands • USER = the user is prompted with a list of all currently active devices and is asked to confirm their addition to the UCM security domain • AUTO = The credentials for the user accounts assigned the necessary role are cached on the Call Server so that they can be sent at a later time to any device that the Call Server requires to join the UCM security domain	basic-6.00
SECURITY DOMAIN STAT	Display the IP address and fingerprint of the UCM Primary Security Server.	basic-6.00
STAT ESALO	Display ESALO information	basic-5.00
STAT IPMG [<supl shelf>]	Display the detailed status of all/one IPMG(s) configured on the system	basic-5.00
STAT IPMG SUMMARY	Display the summary status of all IPMGs configured on the system. .	basic-5.00
STAT L3VPN [side]	Display the VPN tunneling state. Where: Side = 0 / 1 (number of the core)	basic-5.00

Command	Description	Pack/Rel
STAT NTP	Check status of NTP. Status information displays in four categories—current NTP configuration, last NTP configuration, last synchronization error, and counters—and includes the following fields: • NTP enabled or disabled (if disabled, the report includes no further information) • IP addresses of the primary and secondary NTP servers • local time zone offset from UTC • time difference (delta) between system time and NTP server • current threshold level: Minimal, Warning, Maximum • secure mode of operation set to secure or insecure • packets sent • packets received **Note:** NTP status information also appears on the Date and Time page in Element Manager, under the Network Time Protocol field. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	basic-5.00
STAT RFC2833 <TN>	Display RFC2833 capability for TN for selected <TN>.	basis-5.0
STAT SHELLS SECURE	Indicates whether secured shell access is enabled or disabled.	basic-4.50
STAT SHELLS INSECURE	Indicates whether unsecured shell access is enabled or disabled.	basic-4.50
STAT SNMPCONF		basic-6.00

Command	Description	Pack/Rel
	Display the status of the SYNC SNMPCONF command. The result indicates whether the SNMP parameters configured through LD 117 ("OVLY 117 Configuration") are synchronized with the CS. There are two possible results: • SNMP Configuration is in progress When SNMP parameters are added or modified in overlay 117 and the SYNC SNMPCONF command is not executed, the new SNMP parameters are pending activation. • SNMP Configuration is completed When SNMP parameters are added or modified in overlay 117 and the SYNC SNMPCONF command is executed (new SNMP parameters are activated).	
STAT TRANSFERS INSECURE		basic-6.00
	Display the status of the insecure File Transfer Protocol (FTP).	
STAT TRANSFERS SECURE		basic-6.00
	Display the status of the secure File Transfer Protocol (SFTP).	
STAT UCM SYS		basic-6.00
	Show UCM registration status for all system elements.	
STAT UCM SYS REFRESH		basic-6.00
	Request UCM registration status update from all devices.	
STAT UCMSECURITY		
	Show the Primary Security Server IP address and fingerprint	
STAT VOLO	Display the active VOLO TN information	
STAT ZALT <zone>		basic-4.50
	Display Alternative Routing Status, where: zone = bandwidth zone	
STAT ZBR [<zone>]		

Command	Description	Pack/Rel
	Display status of branch office zones, where: zone = bandwidth zone **Note:** With release 4.50 this command supports Alternative Routing for NBWM.	basic-4.00 basic-4.50
SSH KEY ACTIVATE ACTIVE/INACTIVE	Activates / Inactivates the pending SSH key by restarting the SSH server	basic-5.00
SSH KEY ACTIVATE CABINET n/ALL	Activates the pending SSH key on Cabinet n or ALL Cabinet by restarting the SSH server	basic-5.00
SSH KEY CLEAR	Clears all stored public keys from memory, allowing connections to known devices with new public keys.	basic-5.00
SSH KEY CLEAR ACTIVE/ INACTIVE	Clears all stored public keys from memory, allowing connections to known devices with new public keys.	basic-5.00
SSH KEY CLEAR CABINET n/ ALL	Clears all stored public keys from memory, allowing connections to known devices with new public keys.	basic-5.00
SSH KEY GENERATE	Regenerate the keys on the specified device, if no device is specified then the system generates the key locally.	basic-5.00
SSH KEY GENERATE ACTIVE/INACTIVE	Regenerate the keys on the specified device, if no device is specified then the system generates the key locally.	basic-5.00

Command	Description	Pack/Rel
SSH KEY GENERATE CABINET n/ALL	Regenerate the keys on the specified device, if no device is specified then the system generates the key locally.	basic-5.00
SSH KEY SHOW	Displays the key fingerprint for the specified device, and the date the key was generated. If no device is specified then the system shows the key finger print for the local device.	basic-5.00
SSH KEY SHOW ACTIVE/ INACTIVE	Displays the key fingerprint for the specified device, and the date the key was generated. If no device is specified then the system shows the key finger print for the local device.	basic-5.00
SSH KEY SHOW CABINET n/ ALL	Displays the key fingerprint for the specified device, and the date the key was generated. If no device is specified then the system shows the key finger print for the local device.	basic-5.00
STIP DTLS <Node> <Connection_Type> <DTLS_Capability>	Display IP Phones based on signaling encryption related values, namely the type of connection currently in use by each IP Phone and their capability to make DTLS connections. Where: • <Node> = the node ID of the node the subject IP phones belong to, or “ALL” to omit node-based filtering • <Connection_Type> = type of signaling encryption used - INSECURE = no signaling encryption - SECURE” = USec or DTLS - DTLS = DTLS - USEC = UNIStim Security - ALL = all encryption types • <DTLS_Capability> = capability to make DTLS connections - YES = able to make DTLS connections - NO = not able to make DTLS connections	basic-6.00

Command	Description	Pack/Rel
	- ALL = both capabilities	
STIP FW	Print the number of registered IP Phones with associated RLM data	basic-4.50
STIP FW <XX> [<A>] [<BB>] [<FF>]		basic-4.50
	Print the RLM data for registered IP Phones, where: • XX = firmware ID • A = major version designator • BB = minor version designator • FF = filter to apply on firmware version, where: - (==) = equal to - != = not equal to - < = less then - > = greater then	
STIP MODL <MMMM>		basic-4.50
	Print the RLM for all IP Phones, where: MMMM = IP Phone model	
STOP NTP BACKGROUND		basic-5.00
	Stop background synchronization from running. **Note:** You cannot stop a background synchronization if no background routine is running. Attempts to do so result in an error message. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	
SYNC NTP <Manual | BACKGROUND>		basic-5.00
	Synchronize with NTP server in manual or background mode.	

Command	Description	Pack/Rel
	Note: Manual synchronization places LD 117 on hold for 15 seconds. During that time, you cannot abort from the overlay. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	
`TEST ALARM [aaaa nnnn]`	Generate an alarm. Where: • aaaa = any character sequence. However, to test how an existing system message category (for example, BUG, ERR, INI) appears in an alarm browser, use an existing system message. • (nnnn)= any numeric sequence Defaults to 0000. The output shown on the TTY is the system message used as the parameter. The actual trap sent to the trap destination list has the same severity as an existing message defined in the EDT and EPT. Nonexistent system messages have a severity of `Info` . The following items are found in the details section of the trap output: • `commonMIBDateAndTime` = the time when the test is generated • `commonMIBSeverity` = defined by the EDT and EPT or Info(5) • `commonMIBComponentID` = the configured value of the Navigation system name: Navigation site name: CS (component type) • `commonMIBNotificationID` = 0 • `commonMIBSourceIPAddress` = IP Address of Call Server • `commonMIBErrCode` = AAAA NNNN • `commonMIBAlarmType` = 8 (indicating unknown)	basic-4.0 0

Command	Description	Pack/Rel
	• commonMIBProbableCause = 202 (indicating unknown) • commonMIBAlarmData = Contains textual description The rest of the variable bindings are NULL.	
UNREGISTER UCMSECURITY DEVICE	Remove the Primary Security Server mutual trust information from system for the element.	
UNREGISTER UCMSECURITY SYSTEM	Remove the Primary Security Server mutual trust information from system for all system elements.	
UPDATE DBS	Rebuild INET database and renumber host and route entry ID (update network database). **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	

Alphabetical list of Maintenance commands

Maintenance commands share the same entry format as Administration commands.

Command	Description	Pack/Rel
DIS BUF ALL	Disable buffering for all data types	
DIS BUF CDR	Disable buffering for CDR data	
DIS BUF STN	Disable DBA buffering for Station Fast Sync	
DIS BUF TRF	Disable buffering for TRF data	
DIS DBK	Display database disaster recovery's backup & restore	

Command	Description	Pack/Rel
DIS DVLA IDLELOGOUT	Automatic Idle DVLA IP Phones Logout is disabled	
DIS HOST n	Remove a host from the run time host table, where n = host entry number. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
DIS MEDS	Disable Mediation Server Selection feature	
DIS PPP	Disable Point-to-point Protocol access (this enables PPPD)	
DIS ROUTE n	Remove a route from the run time routing table, where n = route entry number. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
DIS ZALT <zone>	Disable ACR for zone, where: • zone = 0–255 • zone = 0–8000 **Note:** Branch Office is configured at the Main Office	basic-4.50 basic-7.00
DIS ZBR <Zone> [ALL] [LOC] [ESA] [TIM] [ALT]	Disable a Zone's Branch Office behaviour, if no specific features are specified, then ALL is assumed, where: • zone = 0–255 • zone = 0–8000 • ALL = all features • LOC = Local Dialing Access	basic-4.00 basic-7.00 basic-4.50

Command	Description	Pack/Rel
	• ESA = Emergency Service Access • TIM = Time Adjustment • ALT = Alternate Routing for Branch	
DIS ZCAC <Zone>		zcac-4.50
	Disable Call Admission Control (CAC) for the identified zone, where: • Zone = 0–255 • Zone = 0–8000 **Note:** Disables the feature on a zone by zone basis.	zcac-7.00
DIS ZONE <x...x>		
	Disable a Zone, No new calls is established inside the disabled zone, from or towards this Zone.	
DVLA LOGOUTLIST <fileName>		basic-7.00
	Parses the specified file from /e/temp/ directory on Call Server and logs out all DVLA IP Phones whose TNs are presented in the file. The file must contain only the TN in string format (for example, 096 0 00 30) on each line.	
DVLA LOGOUTALL [<idleTime>]		basic-7.00
	Logs out all DVLA logged-on idle IP Phones which are idle for more than idleTime minutes (if specified).	
DVLA LOGOUTTN <loop><shelf><card><unit>		basic-7.00
	Logs out a specific DVLA IP Phone if it is logged in and idle.	
ENL BUF ALL	Enable buffering for all data types	
ENL BUF CDR		
	Enable buffering for CDR data	
ENL BUF STN		
	Enable DBA buffering for Station Fast Sync	

Command	Description	Pack/Rel
ENL BUF TRF	Enable buffering for TRF data	
ENL DBK	Enable database disaster recovery's backup and restore	
ENL DVLA MIDNLOGOUT nnnn	Enable Automatic DVLA IP Phones Logout during Midnight Routine. DVLA IP Phone will be logged-out if it is inactive more then nnnn minutes, where: nnnn = 1- (30) - 1440 minutes	basic-7.00
ENL HOST n	Add a host to run time host table, where n = host entry number. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
ENL MEDS	Enable Mediation Server Selection feature	
ENL PPP	Enable Point-to-point Protocol access (Enables PPPD command)	
ENL ROUTE n	Add a route to run time routing table, where n = route entry number . **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
ENL ZALT <zone>	Enable ACR for zone, where: • zone = 0–255 • zone = 0–8000 **Note:** Branch Office zone is configured at the Main Office	basic-4.50 basic-7.00

Command	Description	Pack/Rel
ENL ZBR <zone> [ALL] [LOC] [ESA] [TIM] [ALT]	Enable a Zone's Branch Office behaviour, if no specific features are specified, then ALL is assumed, where: • zone = 0–255 • zone = 0–8000 • ALL = all features • LOC = Local Dialing Access • ESA = Emergency Service Access • TIM = Time Adjustment • ALT = Alternate Routing for Branch	basic-4.00 basic-7.00 basic-4.50
ENL ZCAC <Zone>	Enables Call Admission Control (CAC) for the identified zone, where: • Zone = 0–255 • zone = 0–8000 **Note:** Enables the feature on a zone by zone basis.	zcac-4.50 zcac-7.0
ENL ZONE <x...x>	Enable a Zone	
PING	Ping an IP address to test the network settings. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
PRT DVLA IDLELOGOUT	Print the status of Automatic Idle DVLA IP Phones logout	basic-6.00
SET ENABLE_TRAPS (ON) | OFF C	Enable/disable the sending of SNMP traps. Where:	basic-6.00

Command	Description	Pack/Rel
	• ON = enabled • OFF = disabled	
SET HSP_IP	Activates the HSP IP addresses and subnet mask **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	basic-4.50
SET MASK	Set ELNK subnet mask to configured value (set runtime subnet mask to the configured value). **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
SET MGMT_ALARM	Generate MGMT SNMP Traps	
SET OPEN_ALARM <slot> <IP address> [<port>]	Add an SNMP (Simple Network Management Protocol) trap destination. Where: • <slot> = 0-7 • <IP Address> = any valid value in an x.x.x.x format (TCP/IP) • <port> = destination port for the SNMP trap **Note:** When <port> is not specified, SNMP traps are routed to port 162 by default. **Note:** To clear an SNMP trap destination, specify appropriate <slot> value and set <IP Address> = 0.0.0.0.	
	When SNMP open alarm trap destinations are added or modified in LD117, they are stored in an "OVLY 117 Configuration" area pending activation. When the SYNC SNMPCONF	basic-6.00

Command	Description	Pack/Rel
	command is executed, the "OVLY 117 Configuration" SNMP open alarm changes are activated and become part of the "ACTIVE Configuration" (current) on the system.	
SET USN	Set the unique system name for IP Peer System	
STAT AUTONEG IPM	Display auto-negotiate status of Main Cabinet ports. The following report is displayed: AUTO-NEGOTIATE LINK PARTNER STATUS - MAIN/ CALL SERVER PORTS ---------- PORT Bandwidth Duplex Mode AutoNegotiate ========== IPR 1 UNKNOWN UNKNOWN ON IPR 2 UNKNOWN UNKNOWN IPR 3 100 Mbps full duplex ON IPR 4 UNKNOWN UNKNOWN If the auto-negotiation process is successful, it returns " 100 Mbps full duplex". Otherwise UNKNOWN is reported, indicating a failure in negotiating 100 Mbps full duplex bandwidth.	
STAT AUTONEG IPR	Display auto-negotiate status of Expansion Cabinet ports. The following report is displayed: AUTO-NEGOTIATE LINK PARTNER STATUS - EXPANSION/MEDIA GATEWAY PORTS ---------- PORT Bandwidth Duplex Mode AutoNegotiate ========== IPR 1 UNKNOWN UNKNOWN ON IPR 2 UNKNOWN UNKNOWN IPR 3 100 Mbps full duplex ON IPR 4 UNKNOWN UNKNOWN If the auto-negotiation process is successful, it returns " 100 Mbps full duplex". Otherwise UNKNOWN is reported, indicating a failure in negotiating 100 Mbps full duplex bandwidth.	
STAT BUF	Display buffer info (data type,% full, not ready)	
STAT DBK	Display status of disaster recovery (enabled, disabled)	
STAT ELIN [ALL] / <erl>	Print current status of all ELINs in all / specified ERLs.	basic-5.00

Command	Description	Pack/Rel
STAT ELIN ACTIVE [<erl>]	Print active mappings for specified ERL, or all ERLs if none is specified.	basic-5.00
STAT HOST	Display current runtime host table status (enabled hosts). **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
STAT IP DTLS	Display the Resource Locator Module information for the specified UNIStim encr. and DTLS cap	
STAT IP FW	Display the Resource Locator Module information for Ethersets with specified F/W ID(s)	
STAT IP HOSTIP	Display the Resource Locator Module information corresponding to the specified HOST IP	
STAT IP MODL	Display the Resource Locator Module information for Ethersets of the specified Model Name	
STAT IP NODE	Display the Resource Locator Module information for the specified node	
STAT IP SIPLUA	Display the Resource Locator Module information for SIPL TNs with matching User Agent ID	
STAT IP TERMIP	Display the Resource Locator Module information corresponding to the specified Etherset IP	
STAT IP TN	Display the Resource Locator Module information for the specified TN or group of TNs	
STAT IP TYPE	Display the Resource Locator Module information for the specified TN type	

Command	Description	Pack/Rel
STAT IP ZONE	Display the Resource Locator Module information for the specified zone	
STAT ISET ALL	Display the Resource Locator Module information for all nodes	
STAT ISET NODE	Display the Resource Locator Module information for the specified node	
STAT LINK APP <applicationType>	Display the link information status of the server for the specified application, where: applicationType, where: - LTPS = Line TPS - VGW = Voice Gateway - H323 = H.323 Virtual Trunk - GK = GateKeeper - MC32S = 32 port Mindspeed VGMC	
STAT LINK IP <IP address>	Display the link information status of the server for the specified IP address, or IP addresses of the specified sub-net, where: IP address = the ELAN IP address of the Signaling Server or Voice Gateway Media Card **Note:** The IP address can be in full or partial IP address format. For example, "10.11.12.13" or "10.11".	
STAT LINK NAME <hostName>	Display the link information status of the servers based on the supplied host nam, where: hostName = MAINSERVER	
STAT LINK NODE <nodeID>		

Command	Description	Pack/Rel
	Display the link information status of the specified node, where: nodeID = 0-9999 **Note:** The nodeID identifies the node number assigned to a group of Voice Gateway Media Cards and Signaling Server equipment.	
`STAT LINK SRV <serverType>`	Display the link information status of the servers for the specified server type, where: serverType, is: - ITGP = ITG Pentium - SMC = Media Card - SS = Signaling Server - MC32S = 32 port Mindspeed VGMC	
`STAT PPP`	Display Point-to-point Protocol connection status.	
`STAT ROUTE`	Display host and network routing tables. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
`STAT SERV APP <applicationType>`	Display the link information status of the server for the specified application, where: applicationType is: - LTPS = (Line TPS) - VGW = Voice Gateway - H323 = H.323 Virtual Trunk - GK = GateKeeper - SIP (Session Initiated Protocol)	

Command	Description	Pack/Rel
	- MC32S = 32 port Mindspeed VGMC - SLG = SIP Lines Gateway	
STAT SERV IP <IP address>	Display the link information status of the server for the specified IP address, or IP addresses contained in the specified sub-net, where: IP address = the ELAN IP address of the Signaling Server or Voice Gateway Media Card. **Note:** The IP address can be in full or partial IP address format. For example, "10.11.12.13" or "10.11".	
STAT SERV NAME <hostName>	Display the link information status of the servers based on the supplied host name, where: hostName = MAINSERVER	
STAT SERV NODE <nodeID>	Display the link information status of the specified node, where: nodeID = 0-9999 **Note:** The nodeID identifies the node number assigned to a group of Voice Gateway Media Cards and Signaling Server equipment.	
STAT SERV TYPE <serverType>	Display the server information of the specified server type, where: serverType is: - ITGP = ITG Pentium - SMC = Media Card - SS = Signaling Server - MC32S = 32 port Mindspeed VGMC	

Command	Description	Pack/Rel
STAT SS	Display the server information of the specified Signaling Server.	
STAT UCM SYS		basic-6.00
	Show UCM registration status for all system elements.	
STAT UCM SYSREFRESH		basic-6.00
	Request UCM registration status update from all devices.	
STAT ZBR [<Zone>]		
	Display status of branch office zones, where: • Zone = 0–255 • Zone = 0–8000	basic-7.00
STAT ZONE [<Zone>]		
	Display zone status table, where: • Zone = 0–255 • Zone = 0–8000	basic-7.00
STIP ACF	Displays status for all ACF calls	basic-4.50
STIP ACF <status>		basic-4.50
	Displays Active Call Failover (ACF) status information, where: • UNREG = unregistered calls • HREG = half-registered calls • REB = rebuilt calls • HREB = half-rebuilt calls • PREB = partial-rebuilt calls	
STIP DVLA [<idleTime>]		basic-7.00
	Outputs information (TN, Prime DN, idle time) about logged-in DVLA IP Phones which are idle for more than idleTime minutes (if specified). Not more than 1000 records can be output at once. If more than 1000 records are collected, then Info message SCH2376 is printed.	
STIP HOSTIP <IP address>		

Command	Description	Pack/Rel
	Display information contained in the resource locator module table corresponding to the specified HOSTIP address, or HOSTIP addresses contained in the specified sub-net, where: IP address = the ELAN IP address of the Signaling Server or Voice Gateway Media Card. **Note:** IP address can be in full or partial IP address format. For example, "10.11.12.13", or "10.11".	
`STIP NODE <nodeID>`	Display information contained in the resource locator module table corresponding to the specified node ID, where: nodeID = 0-9999 **Note:** The nodeID identifies the node number you have assigned to a group of VGMC and Signaling Server equipment.	
`STIP SIPLUA <UA string>`	Display SIP Line Services TNs with the specified User Agent string.	basic-6.00
`STIP TERMIP <IP address>`	Display information contained in the resource locator module table corresponding to the specified TERMIP address, or TERMIP addresses contained in the specified sub-net, where: IP address = the TLAN IP address of the IP Phone or Voice Gateway Media Card. **Note:** IP address can be in full or partial IP address format. For example, "10.11.12.13", or "10.11".	
`STIP TN <l s c u>`	Display the resource locator module information for the specified TN, or group of TNs, as denoted by the l s c u and c u parameters.	

Command	Description	Pack/Rel
STIP TYPE <aaa>		
	Display the resource locator module information for the specified TN type. Where valid values for <aaa> are: • I2002 = IP Phone 2002 • I2004 = IP Phone 2004 • I2050 = Avaya 2050 IP Softphone • ISET = all IP sets • VGW = Voice Gateway resources • IPTI = Virtual Trunk and IP Trunks • MC32S = 32 port Mindspeed VGMC	
	Where valid values for <aaa> are: • 1210 = Avaya 1210 IP Deskphone • 1220 = Avaya 1220 IP Deskphone • 1230 = Avaya 1230 IP Deskphone	basic 5-5
	Note: Up to 3 TN types can be specified.	
STIP ZONE <zone>		
	Display the resource locator module information for the specified zone number, or range of zones, where: • zone = 0–255 • zone = 0–8000	basic-7.00
TEST ALARM [aaaa nnnn]		basic-4.00
	Generate an alarm. Where: • aaaa = any character sequence. However, to test how an existing system message category (for example, BUG, ERR, INI) appears in an alarm browser, use an existing system message. • (nnnn)= any numeric sequence Defaults to 0000. The output shown on the TTY is the system message used as the parameter. The actual trap sent to the trap destination list has the same severity as an existing message defined in the EDT and	

Command	Description	Pack/Rel
	EPT. Nonexistent system messages have a severity of `Info` . The following items are found in the details section of the trap output: • `commonMIBDateAndTime` = the time when the test is generated • `commonMIBSeverity` = defined by the EDT and EPT or Info(5) • `commonMIBComponentID` = the configured value of the Navigation system name: Navigation site name: CS (component type) • `commonMIBNotificationID` = 0 • `commonMIBSourceIPAddress` = IP Address of Call Server • `commonMIBErrCode` = AAAA NNNN • `commonMIBAlarmType` = 8 (indicating unknown) • `commonMIBProbableCause` = 202 (indicating unknown) • `commonMIBAlarmData` = Contains textual description The rest of the variable bindings are NULL.	
`TEST SUBNETLIS <IP address>`	Return the location data for the subnet entry that matches the specified IP address.	basic-5.00

Chapter 32: LD 135: Core Common Equipment Diagnostic

LD 135 provides diagnostic and maintenance information. It provides a means of performing the following functions:

- clearing minor and major alarms
- clearing and printing maintenance display contents for the primary Core
- testing the idle Core
- displaying CP/CP PII card status and ID
- enabling and disabling CNI/cCNI cards
- displaying CNI/cCNI card ID and status
- testing SIMMs, inactive CNIs/cCNIs, and standby Core during daily routines
- switch Cores when in redundant mode
- during midnight routines checks primary CNIs/cCNIs, checks for Core redundancy, and attempts to switch Cores

When a status appears disabled, one or more Out-of-Service (OOS) messages may appear. Listed below are the possible OOS messages. (What actually appears are the numbers associated with the OOS text).

Possible OOS messages

0 = CP/CP PII local bus parity threshold exceeded 1 = CP/CP PII card HPM timeout threshold exceeded 8 = Unconfigured CNI/cCNI card 9 = Port has been disabled by craftsperson 10 = Device is not accessible 16 = CNI to 3PE cable 1 on specified card and port lost 17 = CNI to 3PE cable 2 on specified card and port lost 18 = 3PE power lost 19 = 3PE has been manually disabled 20 = CNI/cCNI card has been manually disabled 21 = Card test failed 22 = Port test failed 23 = Extender disabled by Meridian 1 initialization 24 = Port interrupt line 0 disabled 25 = Port interrupt line 1 disabled 26 = Port interrupt line 2 disabled 27 = Port interrupt line 3 disabled 28 = CNI to 3PE cable lost on CPP system

Adding a group to an Option 81C/81C CPII

Note:

Refer to *Avaya CS 1000M and Meridian 1 Large System Upgrades Overview, NN43021-458* to add a group, or groups, to an Option 81C/81C CP PII equipped with Fibre Network Fabric.

Basic commands

CDSP	Clear maintenance displays
CLR GR	Clear secondary system ACTIVE state. Triggers repetitive attempts to redirect all the IP Phones to the primary system for a maximum period defined by FCT. If the primary system is operational, N then falls below GRTHR. (FCT and GRTHR are set in LD 117.)
CMAJ	Clear major alarm, and reset power fail transfer
CMIN	Clears minor alarm for all customers.
CMIN ALL	Clears minor alarm for all customers.
CUTOVR	Transfer call processing from active core to standby core
DIS CNI	Disable all CNIs
DIS CNI c s	Disable the CNI card
DIS CNI c s p	Disable the CNI port
DIS EXT x	Disable the specified extender pair X (0G0 to 0G7, 1G0 to 1G7)
DIS SUTL	Disable System Utility card card at the specified side and slot #
DSPL	Get contents of maintenance display for the active Core
DSPL ALL	Get contents of maintenance display for the active Core as well as previous 63 displays
ENL CNI c s	Enable CNI card
ENL CNI c s p	Enable CNI port
ENL EXT x	Enable the specified extender pair X (0G0 to 0G7 and 1G0 to 1G7)
ENL SUTL	Enable System Utility card at the specified side and slot #

IDC CNI s	Print the card ID for the CNI on the active side
IDC CPU	Print card ID for the active Core
JOIN	Performs the following actions: • Restores redundancy to a system put in single mode by the SPLIT command. • Synchronizes the processor's memory and drives. **Note:** This command CANNOT be used unless the system is already in single mode (SPLIT). **Note:** This command MUST be entered by the I/O port on the active processor.
MIDN	Run midnight routines after LD 135 is aborted and TTY is logged out
SCPU	Switch Cores
SPLIT	Put a redundant (shadowed) system into single (non-shadowed) mode
STAT CNI	Get the status of all configured CNIs
STAT CNI c	Get the status of all configured CNIs from side c
STAT CNI c s	Get the status of all configured CNIs from side c and slot s
STAT CNI c s p	Get the status of port p of the configured CNI from side c and slot s
STAT CPU	Get the status and core numbers for both CPs
STAT EXT	Output all extender pair designations (0G0 to 0G7 and 1G0 to 1G7)
STAT HEALTH	Display Tier 1 and 2 health counts and the status of the hardware components that do not have a health weight.
STAT HEALTH AML	Display the health count of the configured ELAN connections to AML applications.
STAT HEALTH ELAN	Display Tier 2 health count.
STAT HEALTH HELP	Display the meaning of the mnemonics used for the hardware components.
STAT HEALTH HW	Display Tier 1 health count and the status of the hardware components that do not have a health weight.

STAT HEALTH IPL

Display the health count of the IPL connections.

STAT HEALTH VPNTNL

Display the VPN tunnel health.

STAT GR — Print current status of 1+1 Geographic Redundancy on the specified system.

STAT MEM — Get status of SIMMs on both CPs

STAT MEM c m — Get status of SIMMs on both CPs

STAT SUTL — Get status of System Utility (both main and transition) cards

TEST CNI c s — Test cCNI cards (core, slot)

TEST CNI c s p — Test the CNI port

TEST CPU — Test the inactive (standby) Core. This command performs NO tests upon the active (primary) Core. On CPP, no tests are performed, and both active and (if available) redundant CP status and memory are displayed.

TEST GR l s c u

Activate selective test for the IP Phone specified by TN, l s c u.

- Registration for an idle IP Phone is dropped immediately.
- Registration for an IP Phone on an established calls is dropped when the call is disconnected and the IP Phone becomes idle.
- Only one IP Phone can be tested at one time. If a Selective Test is already running on another IP Phone, this command switches the test to the new specified IP Phone.

TEST GR CLR — Clear total or selective test. IP sets re-register to the primary system. No active calls are dropped.

TEST IPB — Test the backplane protocol on the secondary (inactive) Interprocessor Bus. This command does NOT test the primary (active) IPB.

TEST LCD — Test the LCD display on the active CP card.

TEST LEDs — Test LEDs

TEST SUTL — Test System Utility (both main and transition) cards

Alphabetical list of commands

Command	Description	Pack/Rel
CDSP	Clear maintenance displays. This command sets the maintenance display for the primary CP to blank.	basic-18
CLR GR	Clear secondary system ACTIVE state. Triggers repetitive attempts to redirect all the IP Phones to the primary system for a maximum period defined by FCT. If the primary system is operational, N then falls below GRTHR. (FCT and GRTHR are set in LD 117.)	grprim-4.0
CMAJ	Clear major alarm, and reset power fail transfer	basic-18
CMIN	Clears minor alarm for all customers.	alrm_filter-22
CMIN ALL	Clears minor alarm for all customers.	basic-18
CUTOVR	Transfer call processing from active core to standby core	cpp_cni-25
DIS CNI	Disable all cCNIs	cpp_cni-25
DIS CNI c s	Disable the cCNI card. Where: • c = Core number (0 or 1) This must be the standby side. Disable the active side if the CNI is not in service. • s = Slot number (8-12)	cpp_cni-25
DIS CNI c s p	Disable the cCNI port. Where: • c = Core number (0 or 1) This must be the standby side. Disable the active side if the cCNI is not in service. • s = Slot number (8-12) • p = Port number (0, 1) If the P is not entered, both ports, and the card itself are disabled. Where: p = (0, 1, 2) System with Fibre Network Fabric	basic-18 fnf-25
DIS EXT x	Disable the specified extender pair X (0G0 to 0G7, 1G0 to 1G7). Only extenders on the non-active CPU may be disabled. The extender is marked as unusable by the	fnf-25

Command	Description	Pack/Rel
	system and it will not attempt to use it i.e. a CPU changeover will not be permitted.	
DIS SUTL c s	Disable System Utility card. Where: • c = Core number (0 or 1) • s = Slot number (15)	cpp_cni-25
DSPL	Get contents of maintenance display for the active Core. If the maintenance display is blank, BLANK is output.	basic-18
DSPL ALL	Get contents of maintenance display for the active Core, and previous 63 displays.	basic-18
ENL CNI c s	Enable cCNI card	cpp_cni-25
ENL CNI c s p	Enable cCNI port Where: c = Core number (0 or 1) ; s = Slot number (8-12) ; p = Port number (0 or 1) If the P is not entered, both ports, and the card itself are enabled. A port cannot be enabled if the card is disabled. Enabling the CNI card will also enable the 3 Port Extender.	basic-18
	Where: p = (0, 1, 2) System with Fibre Network Fabric	fnf-25
ENL EXT x	Enable the specified extender pair X (0G0 to 0G7 and 1G0 to 1G7). Only extenders on the non-active CPU may be enabled.	fnf-25
ENL SUTL c s	Enable System Utility card. Where: • c = Core number (0 or 1) • s = Slot number (15)	cpp_cni-25
IDC CNI s	Print the card ID for the CNI on the active side. Where: s = Slot number (8-12). The printout appears in the following format: `x y ppppppppaa rrssss ccccccc` Where: • x = Core number (0 or 1) • y = Slot number (8-12) • pppppppp = PEC code	basic-18

Command	Description	Pack/Rel
	• aa = Attribute code • rr = Release number • ssss = Serial number • cccccccc = Comments (optional)	
IDC CPU	Print card ID for the active Core. The printout appears in the following format: `x y ppppppppp rrssss ccccccc` Where: • x = Core number (0 or 1) • y = Slot number (8-12) • ppppppppp = PEC code • rr = Release number • ssss = Serial number • cccccccc = Comments (optional)	basic-18
IDC SUTL c s	Print cCNI's card ID Where: • c = Core number (0 or 1) • s = Slot number (15)	cpp_cni-25
INI ACTIVE	Warmstart active core. **Note:** • Call from active core • Also warmstarts inactive core after trigger time expiry	basic-5.00
INI INACTIVE	Warmstart inactive core. **Note:** • Call from active core of Redundant system • Call from inactive core of Split system	basic-5.00
INI BOTH	Warmstart both active and inactive core.	basic-5.00

Command	Description	Pack/Rel
	Note: • Call from active core of Redundant system • Invalid command in Split mode	
JOIN	Performs the following actions: • Restores redundancy to a system put in single mode by the SPLIT command. • Synchronizes the processor's memory and drives. **Note:** This command CANNOT be used unless the system is already in single mode (SPLIT). **Note:** This command MUST be entered by the I/O port on the active processor.	cpp_cni-25
MIDN	Run midnight routines after LD 135 is aborted and TTY is logged out.	basic-18

SCPU	Switch Cores.
	This command causes the inactive CP to become active. If the switchover is successful, OK in printed. If it is not successful, an error message is printed.
	If, when attempting to switch CPs, the system determines the currently active side is better than the standby side, a message appears on the TTY:
	`FORCE`
	`Enter <YES> to force SCPU to standby Core x.`
	`Press <Return> to abort SCPU.`
	Entering Yes continues the switch. Entering a Carriage Return <CR> defaults to No and retains the currently active side.
		basic-18

SMGR xx yy	Forces Media Gateway to register on a specified Call Server, where: • xx = specified Call Server. Options for this parameter are PRIM (Primary), ALT1 (Alternate Call Server 1), or ALT2 (Alternate Call Server 2). • yy = cabinet number of the Media Gateway to be switched.	

Command	Description	Pack/Rel
	Note: The GRDRC ABKUP prompt must be configured as SCHD on the primary and alternate system for this command to work.	
SPLIT	Put a redundant (shadowed) system into single (non-shadowed) mode. The active Core remains active. Use this command for parallel reload, and for diagnostics requiring split mode operation. Additionally, the standby (inactive) Core "wakes up" and does a system level INIT. When the command is successful, OK is printed. If it is not successful, an error message is printed. This command has the same effect as putting both Cores into MAINT. If a terminal is connected to the secondary Core's I/O port, OS level startup messages appear as well as INI messages. This is not an error, and is operating according to design. If the disks are not synchronized, the command aborts, and an error message appears.	basic-18
STAT CNI	Get the status of all configured cCNIs.	cpp_cni-25
STAT CNI c	Get the status of all configured cCNIs from side c	cpp_cni-25
STAT CNI c s	Get the status of all configured cCNIs from side c and slot s	cpp_cni-25
STAT CNI c s p		
	Get the status of port p of the configured cCNI from side c and slot s. (This command also prints the Network Group number of both ports on each cCNI.) To get the status of a specific cCNI port, enter the following information. Entering only STAT CNI gets the status for all CNI ports. Where: c = Core number (0 or 1) ; s = Slot number (8-12) ; p = Port number (0 or 1). If the P is not entered, the status of all ports is printed, where:	basic-18
	p = (0, 1, 2) System with Fibre Network Fabric	fnf-25
	If the status is DSBL (Disabled), one or more of the OOS reasons may appear. What actually appears are the numbers associated with the OOS text. • 0 = CP local bus parity threshold exceeded • 1 = CP card HPM timeout threshold exceeded	

Command	Description	Pack/Rel
	• 8 = Unconfigured cCNI card • 9 = Port has been disabled by craftsperson • 10 = Device is not accessible • 16 = CNI to 3PE cable 1 on specified card and port lost • 17 = CNI to 3PE cable 2 on specified card and port lost **Note:** 16 and 17 are not applicable for CP PII • 18 = 3PE power lost • 19 = 3PE has been manually disabled • 20 = cCNI card has been manually disabled • 21 = Card test failed • 22 = Port test failed • 23 = Extender disabled by Meridian 1 initialization • 24 = Port interrupt line 0 disabled • 25 = Port interrupt line 1 disabled • 26 = Port interrupt line 2 disabled • 27 = Port interrupt line 3 disabled. • 26 = Port interrupt line 1 disabled • 28 = cCNI to 3PE cable on specified card and port lost	cpp_cni-25
STAT CPU	Get the status and core numbers for both CPs. Possible responses are: • `ENBL` = CP is running • `IDLE` = CP is in standby • `DSBL` = CP is disabled If the status is DSBL, one of the following OOS reasons is printed: • 0 = CP card local bus parity threshold exceeded • 1 = CP card sanity timeout threshold exceeded • 10 = Secondary CP is not accessible • 16 = Secondary CP has a major fault This command also prints out the results of the latest self-test, and the position of the MAINT/NORM switch.	basic-18

Command	Description	Pack/Rel
STAT EXT	Output all extender pair designations (0G0 to 0G7 and 1G0 to 1G7).	fnf-25
STAT EXT x	Output status of the specified ext pair X x = 0G0 from CPU0 to Network Group 0. x = 0G1 from CPU0 to Network Group 1. x = 0G2 from CPU0 to Network Group 2. x = OG3 from CPU0 to Network Group 3. x = OG4 from CPU0 to Network Group 4. x = OG5 from CPU0 to Network Group 5. x = OG6 from CPU0 to Network Group 6. x = OG7 from CPU0 to Network Group 7. x = 1G0 from CPU1 to Network Group 0. x = 1G1 from CPU1 to Network Group 1. x = 1G2 from CPU1 to Network Group 2. x = 1G3 from CPU1 to Network Group 3. x = 1G4 from CPU1 to Network Group 4. x = 1G5 from CPU1 to Network Group 5. x = 1G6 from CPU1 to Network Group 6. x = 1G7 from CPU1 to Network Group 7.	fnf-25
STAT GR	Print current status of 1+1 Geographic Redundancy on the specified system.	grprim-4.0
STAT HEALTH	Display Tier 1 and 2 health counts and the status of the hardware components that do not have a health weight.	basic-3.0
STAT HEALTH AML	Display the health count of the configured ELAN connections to AML applications.	basic-3.0
STAT HEALTH ELAN	Display Tier 2 health count.	basic-3.0
STAT HEALTH HELP	Display the meaning of the mnemonics used for the hardware components.	basic-3.0
STAT HEALTH HW	Display Tier 1 health count and the status of the hardware components that do not have a health weight.	basic-3.0
STAT HEALTH IPL	Display the health count of the IPL connections.	basic-3.0
STAT HEALTH VPNTNL	Display the VPN tunnel health.	basic-5.00

Command	Description	Pack/Rel
STAT MEM	Get the status of SIMMs on both Call Processors. **Note:** On a CoRes Call server, the command does not show the actual physical memory size of the CP PM hardware. It shows the memory size that the Call Server application is using.	cpp_cni-25
STAT MEM c m	Get status of SIMMs on both CPs. To get the status of a single SIMM, or a specific side, enter the following information, where: • c = Core (0 or 1) • m = SIMM number (0-5) If m is not entered, status for all SIMMs is printed. If the status is Disabled (DSBL), the device is not accessible.	basic-18
STAT SUTL	Get status of System Utility, both main and transition cards	cpp_cni-25
SYSLOAD ACTIVE	Coldstart active and inactive core of Redundant system. Coldstart active core of Split system. **Note:** • Call from active core • Resume on previously active core	basic-5.00
SYSLOAD INACTIVE	Coldstart inactive core. **Note:** • Call from active core of Redundant system • Call from inactive core of Split system	basic-5.00
SYSLOAD BOTH	Coldstart active and inactive core of Redundant system. Invalid option in Split mode. **Note:** Call from active core	basic-5.00

Command	Description	Pack/Rel
TEST CNI c s	Test cCNI cards (core, slot)	cpp_cni-25
TEST CNI c s p		basic-18
	Test the cCNI port. Where: • c = Core number (0 or 1) • s = Slot number (8-12) • p = Port number (0 or 1) If the P is not entered, both ports are tested. This command can test Standby cCNIs as well as active cCNIs that are out of service. This may take a few minutes because of the time required to reestablish memory shadowing and contents. When the command is successful, OK is printed. If it is not successful, an error message is printed, where:	
	p = (0, 1, 2) System with Fibre Network Fabric	fnf-25
TEST CPU	Test the inactive (standby) Core. This command performs NO tests upon the active (primary) Core. The CMB (on the CP card), CP to CP cable, and memory are sure that Split mode can be entered safely. Then the CP is tested. The system enters split mode, runs the test, and returns to redundancy (memory shadowing). This may take a few minutes because of the time required to reestablish memory shadowing and contents. It is possible, during the test, that service may be interrupted if an error occurs on the single active Core. Output from this test is " `OK` ," or a CCED message. Refer to the specific message for more information. Testing the secondary (inactive) Core is done by performing a "reset" on the secondary Core. If a terminal is connected to the secondary Core's CPIO, cold start diagnostics are displayed on the terminal. This is not an error, and is operating according to design. **Note:** On CPP, no tests are performed, and both active and (if available) redundant CP status and memory are displayed.	basic-18
TEST GR l s c u		grprim-4.0
	Activate selective test for the IP Phone specified by TN, l s c u.	

Command	Description	Pack/Rel
	• Registration for an idle IP Phone is dropped immediately. • Registration for an IP Phone on an established calls is dropped when the call is disconnected and the IP Phone becomes idle. • Only one IP Phone can be tested at one time. If a Selective Test is already running on another IP Phone, this command switches the test to the new specified IP Phone.	
TEST GR CLR		grprim-4.0
	Clear total or selective test. IP sets re-register to the primary system. No active calls are dropped.	
TEST IPB	Test the backplane protocol on the secondary (inactive) Interprocessor Bus. This command does NOT test the primary (active) IPB. The system enters split mode, runs the test, and returns to redundancy (memory shadowing). When the command is successful, OK is printed. If it is not successful, an error message is printed. This may take a few minutes because of the time required to reestablish memory shadowing and contents. It is possible, during the test, that service may be interrupted if an error occurs on the single active Core.	basic-18
TEST LCD	Test the LCD display on the active CP card. The following test pattern is displayed on the active CP card's display: • 8888888888888888 • 8888888888888888 • ABCDEFGHIJKLMNOP • QRSTUVWXYZ123456 • abcdefghijklmnop • qrstuvwxyz09876 The first two tests go by very quickly, so you may actually see only the third one.	basic-18
TEST LEDs	Test LEDs	cpp_cni-25
TEST SUTL	Test System Utility (both main and transition) cards	cpp_cni-25

Chapter 33: LD 137: Core Input/Output Diagnostic

LD 137 provides IOP, CMDU, and cMMDU related diagnostic and maintenance information. Some commands in LD 37 can also be used. Refer to that program.

LD 137 provides a means of performing the following functions:

- enabling and disabling the IOP, CMDU, and cMMDU cards
- displaying status and card ID for IOP, CMDU, and cMMDU cards
- testing the IOP, CMDU, and cMMDU (the hard and floppy disk drives are tested)
- testing individual disk drives
- enabling and disabling disk redundancy
- testing SCSI cable connections between IOP, CMDU, and cMMDUs
- testing disk synchronization on file or sector levels
- during midnight routines performs DATA CMDU, DATA RDUN commands
- displaying the Security Device Identification of the Security Dongle
- enabling and disabling the ELNK

The DATA CMDU AND DATA RDUN midnight routines are run every 5 days.

When a status appears disabled, one or more Out of Service (OOS) messages may appear. Listed below are the possible OOS messages:

- IOP out-of-service
- Unexpected interrupt fault monitor threshold exceeded
- Fault interrupt fault monitor threshold exceeded
- Processor exception fault monitor threshold exceeded
- ASIC interrupt fault monitor threshold exceeded
- Unrecognized error fault monitor threshold exceeded
- General event interrupt fault monitor threshold exceeded
- IOP not responding
- IOP disabled by craftsperson
- IOP responding but cannot be enabled
- CMDU/cMMDU out-of-service
- Hard disk read error

- Hard disk write error
- Hard disk drive error
- CMDU/cMMDU does not respond, the disk drive may be missing
- CMDU/cMMDU has been disabled by the craftsperson
- CMDU/cMMDU is disabled because the IOP is out-of-service
- Hard disk is inaccessible
- CMDUs/cMMDUs are not synchronized
- CMDU/cMMDU status is mismatched because of a software error
- CMDU/cMMDU is in split mode
- CMDU/cMMDU is out of split mode
- No access to hard disk (HDK)

Basic commands

DATA CMDU n	Perform read tests on the specified CMDU
DATA CMDU n HDK, FDK	
	Perform read test on either the Hard Disk or Floppy Disk
DATA RDUN	Perform sector level checking on both hard disk
DIS CMDU n	Disable CMDU
DIS ELNK	Disable the ethernet link on the active IOP card **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.
DIS IOP	Disable the active IOP and Ethernet
ENL CMDU n	Enable the CMDU
ENL ELNK	Enable the ethernet link on the active IOP card **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.
ENL IOP	Enable IOP on the active Core and Ethernet

ENL HOST n	Add a host to run time host table
IDC	Print the IDs of both CMDUs and the active IOP **Note:** This command is not applicable to CPP systems.
IDC CMDU n	Print the ID for the CMDU
IDC CMDU c s d	Print the ID for the CMDU
IDC IOP	Print out the ID of the active IOP
SDID	Display Security Device Identification
STAT	Get status of IOPs, CMDUs, MMDUs and Ethernet
STAT CMDU n	Get status of the CMDU/MMDU
STAT CMDU c s d	Get status of the MMDU
STAT ELNK	Display status of the ethernet link on the active IOP card whether enabled or disabled (display the current active ELAN information). **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.
STAT HOST	Display current run time host table status
STAT IOP	Display status of the active IOP and Ethernet
STAT RDUN	Get status of both hard disks
SWAP	Swap the CMDUs
SYNC	Synchronize the hard disks on both CMDUs
TEST CMDU n	Perform test for the CMDU
TEST CMDU c s d	Perform test for the MMDU
TEST CMDU n HDK, FDK	Perform test on the Hard or Floppy Disk
TEST IOP	Perform the self test on the active IOP

TEST RDUN	Perform file level checking on both hard disks
TEST SCSI	Test the SCSI cables
TTY x	Test TTY x

Alphabetical list of commands

Command	Description	Pack/Rel
DATA CMDU n		
	Perform read tests on the specified CMDU. This data validity check is performed on both hard and floppy disks. While the test is in progress, the CMDU is inaccessible. Progress messages are output. n = core number (0 or 1) If n is not entered, this command checks both CMDUs. This is more extensive than the TEST command, and may take longer.	basic-18
DATA CMDU n HDK, FDK		
	Perform read test on either the Hard Disk or Floppy Disk. This is a data validity check. While the test is in progress, the Disk is inaccessible. Where: n = Core number (0 or 1). You must enter the Core number. This is more extensive than the TEST command, and may take longer.	basic-18
DATA RDUN	Perform sector level checking on both hard disks. This test ensures that disk synchronization (disk redundancy) exists. It can only be performed when disk redundancy is enabled. All data is checked, on both disks, sector by sector. If the test fails, a CIOD message appears, and disk redundancy is disabled. This is more extensive than the TEST command, and may take longer. While this test is in progress, the disks are inaccessible.	basic-18
DIS CMDU n		basic-18
	Disable CMDU. Where: n = Core number (0 or 1). You must enter the Core number. If disk redundancy is currently enabled (both CMDUs are enabled and enabled), disabling the CMDU also disables disk redundancy.	

Command	Description	Pack/Rel
	The confirmation is displayed: `"CURRENTLY CMDU N IS ACTIVE. DISK RDUN WILL BE DISABLED. ENTER Y(ES) TO CONFIRM, N(O) TO ABORT."` If the specified CMDU is in standby, its state is changed to disabled. If it is the active CMDU, it is disabled, and the standby CMDU becomes active.	
DIS ELNK	Disable the ethernet link on the active IOP card. An attempt is made to disable the Ethernet link. When the link is disabled, all activities will be terminated. The system displays `OK` to indicate that the link is disabled or `FAIL` to indicate that the link could not be disabled. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	basic-22
DIS IOP	Disable the active IOP and Ethernet. The LED is lit on the IOP faceplate and both CMDUs are inaccessible.	basic-18
ENL CMDU n	Enable the CMDU. Where: n = Core number (0 or 1). You must enter the Core number. When the first CMDU is enabled, that CMDU state is ACTIVE. If a second ENL CMDU is attempted, a file level synchronization on both hard disks is performed first. If the synchronization (disk redundancy) does not exist, a CIOD error message is printed, and the second CMDU remains disabled. If the synchronization exists, the confirmation is displayed: `"DISK RDUN WILL BE ENABLED, ENTER Y(ES) to CONFIRM, N(O) TO ABORT."` When disk redundancy is successful, both CMDU states are Enabled. The CMDU enabled first is active, and the second is standby.	basic-18
ENL ELNK	Enable the ethernet link on the active IOP card. If the Ethernet link is down, entering this command will cause an attempt to restore the Ethernet link to normal operation state. However, if the system cannot successfully restore the link, the Ethernet link will remain disabled. If the link was already up, this command does not affect the current operation of it. The system displays `OK` to indicate that	basic-22

Command	Description	Pack/Rel
	the link is now enabled or `FAIL` to indicate that the link could not be enabled. **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
ENL HOST n	Add a host to run time host table.	basic-22
ENL IOP	Enable IOP and Ethernet on the active Core. The LED is turned off on the IOP faceplate. The CMDUs are restored to the state they were in prior to the IOP being changed. However, if the cable between the IOPs is not connected, the CMDUs remain inaccessible until the cable is reattached. If both CMDUs were enabled, a file level synchronization check is performed prior to restoring states. If the synchronization (disk redundancy) does not exist, only the previously active CMDU is enabled.	basic-18
IDC	Print the IDs of both CMDUs and the active IOP. The printout appears in the following format: `pppppppppp rrssss cccccccc` Where: • `pppppppppp` = PEC code • `rr` = Release number • `ssss` = Serial number • `cccccccc` = Comments (not always be present) **Note:** The IDC command is not available for CPP systems.	basic-18
IDC CMDU n	Print the ID for the CMDU. Where: n = Core number (0 or 1). If n is not entered, card ID information is printed for both CMDUs.	basic-18
IDC IOP	Print out the ID of the active IOP.	basic-18

Command	Description	Pack/Rel
SDID	Display Security Device Identification of Security Dongle(s)	basic-23
STAT	Get status of IOPs, CMDUs, MMDUs and Ethernet. For the IOP, the Enabled or Disabled, and Active or Standby state is printed. Status is given for active and standby IOPs. For the CMDU/MMDU, Disk redundancy, enabled/disabled, and active/standby status are printed. If Ethernet is disabled, the status (enabled or disabled) is displayed along with an OOS message. The status given for the standby IOP is a software status as it was last seen when that IOP was active. No hardware status is given because the standby IOP cannot be accessed. If the status of the IOP or CMDU is disabled, one of the following OOS messages may appear: • IOP out-of-service • Unexpected interrupt fault monitor threshold exceeded • Fault interrupt fault monitor threshold exceeded • Processor exception fault monitor threshold exceeded • ASIC interrupt fault monitor threshold exceeded • Unrecognized error fault monitor threshold exceeded • General event interrupt fault monitor threshold exceeded • IOP not responding • IOP disabled by craftsperson • IOP responding but cannot be enabled • CMDU/MMDU out-of-service • Hard disk read error • Hard disk write error • Hard disk drive error • CMDU/MMDU does not respond, the disk drive may be missing • CMDU has been disabled by the craftsperson • CMDU/MMDU is disabled because the IOP is out-of-service • Hard disk is inaccessible: CMDUs are not synchronized • CMDU/MMDU status is mismatched because of a software error • CMDU/MMDU is in split mode	basic-18

Command	Description	Pack/Rel
	• CMDU/MMDU is out of split mode • No access to hard disk (HDK) **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
STAT CMDU n	Get status of the CMDU. Where: n = Core number (0 or 1). If n is not entered, the status for both CMDUs is printed. If the CMDU is disabled, one of the following CMDU OOS reason may appear: • Hard disk read error • Hard disk write error • Hard disk drive error • CMDU does not respond, the disk drive may be missing • CMDU has been disabled by the craftsperson • CMDU is disabled because the IOP is out-of-service • Hard disk is inaccessible • CMDUs are not synchronized • CMDU status is mismatched because of a software error • CMDU is in split mode • CMDU is out of split mode • No access to hard disk (HDK) **Note:** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	basic-18
STAT CMDU c s d	Get status of the MMDU, where: • c = 0 or 1, Core number • s = 16, Slot number • d = 1, Drive number	cpp_cni-25

Command	Description	Pack/Rel
	Note: This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	

STAT ELNK	Display status of the ethernet link on the active IOP card whether enabled or disabled. The Ethernet address of this active Input Output Processor (IOP) is also displayed (display the current active ELAN information).
	Since the Local Area Network Controller for Ethernet (LANCE) is equipped on the IOP, LANCE will be disabled when the IOP is disabled.
	If the ethernet link is disabled, an OOS reason will be displayed containing the following information:
	`ELNK ENABLED`
	`Ethernet (In unit number 0):`
	`Host: aaaxxx`
	`Internet address: xx.xxx.xx.xxx`
	`Netmask: xxxxxxxxxx ; Subnetmask: xxxxxxxxxx`
	`xxx packets received ; xxx packets sent`
	`x input errors ; x output errors`
	`x collisions`
	Note:
	This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.
		basic-22

STAT HOST	Display current run time host table status.	basic-22
STAT IOP	Display status of the active IOP and Ethernet. This command prints out the status whether the IOP is enabled or disabled. If it is disabled, the OOS reasons are printed. The following IOP OOS messages may appear: • IOP out-of-service • Unexpected interrupt fault monitor threshold exceeded • Fault interrupt fault monitor threshold exceeded • Processor exception fault monitor threshold exceeded • ASIC interrupt fault monitor threshold exceeded • Unrecognized error fault monitor threshold exceeded • General event interrupt fault monitor threshold exceeded • IOP not responding	basic-18

Command	Description	Pack/Rel
	• IOP disabled by craftsperson • IOP responding but cannot be enabled	
SWAP	Swap the CMDUs. After this command is issued, the active CMDU becomes standby, and the standby CMDU becomes active. This command is performed only when disk redundancy is enabled.	basic-18
SYNC	Synchronize the hard disks on both CMDUs. This is a sector level synchronization. It is performed by copying the data from the active CMDU to the disabled CMDU, sector by sector. This can only be done when one CMDU is active and one is disabled. The confirmation prompt appears when the system is ready to do the copying: `"CMDU n ACTIVE HDK WILL BE COPIED AND DISK RDUN WILL BE ENABLED. ENTER Y TO CONFIRM."` Synchronization may take as long as 40 minutes. Progress reports appear on the TTY periodically.	basic-18
TEST CMDU n	Perform test for the CMDU. This test includes a self-test, read/write capability test, and disk access test on both hard and floppy disks for this CMDU. While the test is in progress, the CMDU is inaccessible. Where: n = Core number (0 or 1). You must enter the Core number. A disk must be in the floppy drive when this test is run. If the floppy disk is not present, the floppy disk test will fail. The hard disk test will not be affected.	basic-18
TEST CMDU c s d	Perform test for the MMDU, where: • c = 0 or 1, Core number • s = 16, Slot number • d = 1, Drive number	cpp_cni-25
TEST CMDU n HDK, FDK	Perform test on the Hard or Floppy Disk. This test includes a self-test, read/write capability test, and disk access test on either the hard or floppy disk drive for this CMDU. While the test is in progress, the CMDU is inaccessible.	basic-18

Command	Description	Pack/Rel
	Where: n = Core number (0 or 1). You must enter the Core number. A disk must be in the floppy drive to test it. If a floppy disk is not present, the floppy disk test will fail. The hard disk test will not be affected.	
TEST IOP	Perform the self test on the active IOP and internal loop-back test on Ethernet. The IOP must be disabled to perform this test.	basic-18
TEST RDUN		basic-18
	Perform file level checking on both hard disks. This test ensures that disk synchronization exists. It can only be performed when disk redundancy is enabled. If the test fails, a CIOD message appears, and disk redundancy is disabled. While this test is in progress, the disk is inaccessible.	
TEST SCSI	Test the SCSI cables. This test ensures the cable connections between the IOPs are present. Access to the CMDUs is tested as well. If the test is successful, OK is printed. If the test is unsuccessful, CIOD messages are printed to indicate the problem.	basic-18

TTY x	Test TTY x. Response is:
	`ABCDEFGHIJKLMNOPQRSTUVWXYZ`
	`0123456789"#$%*!&()<>—.:,.? READY FOR INPUT`
	Anything entered on the keyboard will be echoed until END is input.
		basic-18

Chapter 34: LD 143: Customer Configuration Backup and Restore

Overlay 143 introduces the Keycode Management feature for customers with the Input/Output Disk Unit with CD-Rom (IODU/C). Previously, a Keycode was stored on two devices: a Security Cartridge and a Direct.rec file.

A Keycode is a "soft" entity that resides on a customer's hard disk. A Keycode can be delivered, replaced, upgraded, and downgraded.

Note:
As of Communication Server 1000 Release 7.0, new ISM limits can be activated without sysload if they are greater than or equal to the actual ISM usage in the system. Otherwise, installation of the new keycode is blocked.

All Keycode Management commands are executed in Overlay 143.

Basic commands

ABORT UPGMG	Aborts all the current and pending centralized software upgrades and disables the automatic software upgrade option.
ABKO	Attended Backup. The new file created to store the MIB-II variables, System Navigation variables, and community name strings is backed up to floppy disks.
ARES	Attended Restore. The new file created to store the MIB-II variables, System Navigation variables, and community name strings is restored from floppy disks.
DIS AUTOUPGMG	Disables the automatic software upgrade option.
ENL AUTOUPGMG <a...a>	Enables the automatic centralized software upgrade option, where: a...a = (SEQ) SIM

HELP	View overlay commands on terminal
KDIF k1 k2	Print the differences between two specified keycodes
KMAN	Manually introduce the keycode the same way as form the Installation Tools
KNEW dr	Check and accept new keycode file
KOUT	Delete "keycode.new" file
KRVR d r	Revert the current keycode.rec and keycode.old files
KSHO k	Show content of the currently used keycode file and the differences with the rest of keycode files
KSTT	Print the status of a new (trial) keycode (if any).
KUPL	Upload keycode command.
MDP ISSP	Prints all inservice patches and patch handle numbers (includes all DepList patches).
PRT AUTOUPGMG	Displays the settings for the automatic upgrade option.
PSDL LIST	List peripheral software download files.
UPGMG x	Upgrades MG 1000S.
UPGMGBOOT	Upgrade MG 1000S with bootROM from Call Server
UPGRADE	Perform Small System, CS 1000S, MG 1000B, and MG 1000T upgrade
UPGUDT l s c	Perform UDT card firmware upgrade
UPGUDTABORT	Abort UDT card firmware upgrade
UPGUDT STAT	Query current UDT card firmware upgrade status
XBK	Remote backup database
XCDR x	CDR file retrieval for Small System, CS 1000S, MG 1000B, and MG 1000T
XRT	Remote restore database

XSL	Remote sysload the system
XVR	Remote verify database

Alphabetical list of commands

Command	Description	Pack/Rel
ABORT UPGMG		
	Aborts all the current and pending centralized software upgrades and disables the automatic software upgrade option.	
	For CS 1000S system	basic-2
ABKO	Attended Backup. The new file created to store the MIB-II variables, System Navigation variables, and community name strings is backed up to floppy disks.	basic-23
ARES	Attended Restore. The new file created to store the MIB-II variables, System Navigation variables, and community name strings is restored from floppy disks.	basic-23
DIS AUTOUPGMG		
	Disables the automatic software upgrade option.	
	For CS 1000S system	basic-2.0
ENL AUTOUPGMG <a...a>		
	Enables the automatic centralized software upgrade option, where: a...a = (SEQ) SIM SEQ: Upgrade to the gateways is performed across the LAN in a sequential manner. One gateway will be upgraded at a time, no other gateway upgrades will be initiated until the current MG 1000S has completed its installation. SIM: Upgrade to the gateways is performed in a simultaneous manner across the LAN. All gateways will be upgraded to at the same time. The following warning will be presented to the installer: "WARNING: Call Processing is not guaranteed to operate on the call server during simultaneous upgrades. Do you wish to proceed? (y/n) " The automatic upgrade option for	

Command	Description	Pack/Rel
	simultaneous operation will be enabled upon the installer entering (y). For CS 1000S system	basic-2
HELP	View overlay commands on terminal	basic-23
KDIF k1 k2	Compare 2 keycodes: Where p1 and p2 have one of the following values: • NEW - pending keycode accepted by means of KNEW command • REC - keycode currently in use disk • OLD - previously used keycode PIV and CP PM CPU only • RMD - candidate keycode on Removable Media Device • FMD - candidate keycode created by means of KMAN/KUPL PII CPU only • F0 - Candidate Keycode on floppy disk /f0 • F1 - Candidate Keycode on floppy disk /f1 • HD - Candidate Keycode on hard disk	basic-23
KMAN	Line-by-line candidate keycode file creation Manually enter the keycode to the target system. Enter 21 lines, 16 characters each. Type “end” and press Enter at line 22 to end the process and save keycode.	
KNEW dr	Select new candidate keycode from: parm. Depending on eligibility, the keycode may be instantly activated or activated on next reset. Instant activation is supported if the new ISM limit is greater than or equal to the actual ISM usage in the system. Otherwise, the keycode activation is blocked. Where parm has one of the following values: PIV and CP PM CPU only • RMD - candidate keycode on Removable Media Device • FMD - candidate keycode created by means of KMAN/KUPL PII CPU only • F0 or F1 - keycode on the floppy drive on Core 1 or Core 0 • HD - candidate keycode hard drive If the system instantly activates the New Keycode, the following message prints: `CCBR020 New Keycode accepted and activated`	basic-23

Command	Description	Pack/Rel
	successfully. Sysload is NOT needed! If the system activation for the New Keycode is blocked due to the new ISM limit being lower than the actual ISM usage in the system, the following message prints: CCBR032 New keycode is not activated because the newly configured ISM limit is less than the actual usage. CCBR005 Failed to submit the new keycode. If the New Keycode cannot be activated instantly, the following message prints: CCBR009 New Keycode accepted. It will be activated during the next restart.	
KOUT	Delete "keycode.new" file.	basic-23
KRVR d r	Select the OLD keycode as the new candidate. Depending on eligibility, the keycode may be instantly activated or activated on next reset. The old keycode is eligible for instant activation with the KRVR command if the only difference between the old keycode and the new keycode is that some or all of the License parameters in the old keycode are higher. After the KRVR command has been entered, the following message is printed if the system has instantly activated the Old Keycode: CCBR020 New Keycode accepted and activated successfully. Sysload is NOT needed!	basic-23
	Select the OLD keycode as the new candidate. Depending on eligibility, the keycode may be instantly activated or activated on next reset. The old keycode is eligible for instant activation with the KRVR command if the only difference between the old keycode and the new keycode is that some or all of the License parameters in the old keycode are higher. Instant activation is supported if the new ISM limit is greater than or equal to the actual ISM usage in the system. Otherwise, the keycode activation is blocked. The old keycode is eligible for instant activation with the KRVR command if the only difference between the old keycode and the new keycode is that some or all of the License parameters in the old keycode are higher or lower than the existing parameters but greater than or equal to the actual License usage in the system.	Basic-7.00

Command	Description	Pack/Rel

	After the KRVR command has been entered, the following message prints if the system instantly activates the Old Keycode:
	`CCBR020 New Keycode accepted and activated successfully.`
	`Sysload is NOT needed!`
	If the system activation for the Old Keycode is blocked, the following message prints:
	`CCBR032 New keycode is not activated because the newly configured ISM limit is less than the actual usage.`
	`CCBR007 Failed to revert to the old keycode`	

KSHO k	Display contents of the pending keycode contents, where parm may have one of the following values: • NEW - pending keycode accepted by means of KNEW command • REC - keycode currently in use • OLD - previously used keycode PIV and CP PM CPU only • RMD - verify keycodes on the Removable Media Device • FMD - verify keycodes on the Fixed Media Device PII CPU only • F0 or F1 - verify keycodes on Core 0 or 1 • HD - Core 1 (CPT)	basic-23
KSTT	List all keycodes: NEW, REC, OLD, RMD, FMD	
KUPL	Candidate and PWs keycode file upload. Upload keycodes to the hard disk or FMD on the target system	
MDP ISSP	Prints all inservice patches and patch handle numbers (includes all DepList patches).	
MDP INSTALL <path/file>	Installs the contents of an MDP patch file on a target system. Deactivates all in-service patches and unloads them from the system. Where <path> is a system folder or RMD device name such as CF2, and <file> is a deplist zip file using the 8.3 file naming convention. For example: MDP INSTALL cf2/deplist.zip.	

Command	Description	Pack/Rel
	Note: If you already have patches in service on the target system for the current software release installed, it is recommended to use the REFRESH command in order to update the PATCH deltas only.	
MDP REACTIVATE	Reactivates MDP patches which have been deactivated as a result of sysload.	
MDP REFRESH <path/file>	Refreshes the MDP patches on a target system. Where <path> is a system folder or RMD device name such as CF2, and <file> is a deplist zip file using the 8.3 file naming convention. For example: MDP REFRESH cf2/deplist.zip First determines deltas between existing patches in service and patches identified in MDP Distribution, and divides them into two categories (add and drop). Before applying patches from add category, conflict checking is done with the existing patches and in case of any conflict, the details of conflicts are displayed, and the refresh process is terminated. If no conflict, the patches identified can be applied at once, or can be deferred until midnight routine of that day or alternate day. First those patches identified for removal are removed, after which the patches to be added are loaded and placed into service. **Note:** This command will generate deltas based on the files that are already present in the patch directory of the system. They are not based on the state of the patch (loaded, in-service, unloaded or out of service). If a patch file of the MDP distribution is already present in the patch directory of the system, this patch file is not copied from the distribution to the system. So the condition of the patch, whether it is in service, loaded, or out of service state, remains the same and is untouched by the MDP REFRESH command.	
MDP REVERT	Reverts to a previously installed MDP patch distribution, taking advantage of the deltas created during the previous refresh.	
MDP UNINSTALL	Removes contents of a previously installed MDP patch distribution from the system. First it deactivates, then removes, all Patches from the system. **Caution:** Use this command with caution.	
PRT AUTOUPGMG	Displays the settings for the automatic upgrade option.	

Command	Description	Pack/Rel
	For CS 1000S system	basic-2
PSDL LIST	List peripheral software download files. The PSDL LIST command displays the M3900 language set currently installed on the switch, and the language sets available on the switch. See example below: <option> : LIST - List M3900 language sets CHANGE - Change M3900 language set RESTORE - Restore M3900 language set <language> : Use with PSDL CHANGE option 1 - Global 10 Languages 2 - Western Europe 10 Languages 3 - Eastern Europe 10 Languages 4 - North America 6 Languages 5 - Spare Group A 6 - Spare Group B .psdl list 3900 language set currently installed on the switch : Release and Issue x112551a VERSION 77 1. Global version : psdl.rec/psdl_1.rec 3900 language sets available on the switch : Release and Issue x112551a VERSION 77 1. Global version : psdl.rec/psdl_1.rec Release and Issue x112551a VERSION 77 2. Western Europe : Release and Issue x112551a VERSION 77 3. Eastern Europe version : Release and Issue x112551a VERSION 77 4. North American version : Release and Issue x112551a VERSION 77 5. Phase I F/W for up-issue : Release and Issue x112551a VERSION 77 6. Copy of North America version	basic-25
UPGMG x	UPGMG <supl shelf> UPGMG <supl shelf> FORCE UPGMG <supl shelf> [CSP|MSP|APP|FPGA|BOOT|DBL1|DBL2] UPGMG <supl shelf> [CSP|MSP|APP|FPGA|BOOT|DBL1|DBL2] FORCE UPGMG ALL [SEQ|SIM] UPGMG ALL [SEQ|SIM] FORCE UPGMG ALL [SEQ|SIM] [CSP|MSP|APP|FPGA|BOOT|DBL1|DBL2] UPGMG ALL [SEQ|SIM] [CSP|MSP|APP|FPGA|BOOT|DBL1|DBL2] FORCE UPGMG STAT UPGMG STAT <supl shelf> UPGMGBOOT <supl shelf> For CS 1000E system	basic-5.0

Command	Description	Pack/Rel
	Immediately initiates a manual upgrade of the version of loadware installed on the Call Server to the specified Media Gateway, through the LAN connection to the Media Gateway. When using the FORCE option, this upgrade occurs even if the version of software on the Media Gateway matches the Call Servers version. WARNING: Call Processing is not guaranteed to continue while the media gateways are being upgraded.	
UPGMG x	Upgrade MG 1000S, where: x = MG 1000S	
	For CS 1000S system	basic-2.0
	Immediately initiates a manual upgrade of the version of software and bootROM installed on the Call Server to the specified MG 1000S via the LAN connection to the MG 1000S. This upgrade occurs even if the version of software on the MG 1000S matches the Call Servers version. The MG 1000S must already have at a minimum CS 1000S release 2 installed, for the command to work. WARNING: Call Processing is not guaranteed to operate on the Call Server if this option is initiated to other MG 1000S systems, while the Call Server is currently upgrading to another MG 1000S.	
UPGMG x		
UPGMG STAT		
UPGMGBOOT x		
	Upgrade MG 1000S with bootROM from Call Server, where: x = MG 1000S	
	For CS 1000S system	basic-2.0
	Immediately initiates a manual upgrade of the current version of the bootROM operating on the Call Server to the selected MG 1000S via the LAN connection to the specified MG 1000S. WARNING: Call Processing is not guaranteed to operate on the Call Server if this option is initiated to other MG 1000S systems, while the Call Server is currently upgrading another MG 1000S.	
UPGRADE	Perform Small System, CS 1000S, MG 1000B, and MG 1000T upgrade. This command invokes the Install Setup Program. To perform an installation, the installer inserts a Software Delivery Card in the PCMCIA slot on the System Core Card. Then, on TTY 0, the installer may invoke the Setup Program by using the UPGRADE command in LD 143.	basic-22

Command	Description	Pack/Rel

	The UPGRADE command allows changes to License parameters to be instantly activated without Sysload upon keycode acceptance. The following message is output:
	`CCBR020 New Keycode accepted and activated successfully.`
	`Sysload is NOT needed!`
	`When feature packages are added to the system, a Sysload must be performed.`	

UPGUDT l s c	Perform UDT card firmware upgrade on [supl shelf card]. If the UDT can not be reached then the following response is printed: Cab [LLL S]: Not available. UDT Upgrade command ignored. If an UDT upgrade is already in progress then the following response is printed: UDT[LLL S CC]: Doing Upgrade already. Upgrade command ignored.	basic-6.00
UPGUDTABORT	Abort UDT card firmware upgrade. If the abort request was made after the UDT has erased it's old firmware then terminating the upgrade will cause the UDT to be left without any upgraded code, and it will load its fixed factory firmware load. When this is the case, to confirm the abort request the Call Server prints the following message: UDT [LLL S CC] is undergoing an upgrade. Do you want to abort the upgrade? ENTER Y(ES) TO CONFIRM ABORT UPGRADE, N(O) TO IGNORE COMMAND. If confirmed, an abort message will be sent to the UDT.	basic-6.00
UPGUDTSTAT	Query current UDT card firmware upgrade status. UPGUDT STAT command reports the current UDT card firmware upgrade state and the TN of the UDT card that is currently upgraded. If no upgrade is currently taking place, the reply is: UDT Upgrade is idle. If a UDT card firmware upgrade is in process, the response format is: UDT Upgrade is [idle / checking / starting / active / aborting]. Loop [LLL S CC]	basic-6.00
XBK	Remote backup database. Backup the configuration files from the primary drive onto a computer.	basic-22
	Remote backup database. Backup the configuration files from the primary drive onto a computer. If the CCBR file exists in the system, the time stamp of the CCBR file prints out prior to printing out the ready transmit prompt. For example, `CCBR file is last archived on WED JAN 20 13:08:10 2010. To update the file, please use the EDD CCBR command in Overlay 43. R>Ready to transmit...` If CCBR	basic-7.00

Command	Description	Pack/Rel
	file does not exist in the system, the following message is printed: `CCBR033 CCBR file is missing. Please generate the CCBR file by means of EDD CCBR in Overlay 43.`	
XCDR x ALL	Small System, CS 1000S, and MG 1000T CDR file retrieval from one or all IP expansions after the expansion restores to slave mode, where: x = 1, 2, 3, or 4, IP expansion When the command is successful, the retrieved file is deleted on the expansion.	sipe-25
XRT	Remote restore database Restore the files from a computer onto the primary drive.	basic-22
XSL	Remote sysload the system Sysload the Small System, CS 1000S, MG 1000B, or MG 1000T system from the primary flash drive.	basic-22
XVR	Remote verify database Verify the files on a computer with the files in the primary flash drive of the Small System, CS 1000S, MG 1000B, or MG 1000T system.	basic-22

Chapter 35: Media Card command line interface commands

Contents

This section contains information on the following topics:

- Introduction on page 540
- Overview on page 540
- ITG-SA command line interface commands on page 541
  - OAM security shell commands on page 541
    - Table 20: OAM CLI command groups on page 542
    - OAM General purpose commands on page 543
    - OAM File transfer commands on page 546
    - OAM IP configuration commands on page 549
    - OAM Reset commands on page 550
    - OAM DSP commands on page 550
    - OAM IP Phone firmware upgrade commands on page 550
    - OAM Shell command on page 552
    - OAM Voice Gateway commands on page 553
    - OAM Data Path Capture Tool commands on page 553
    - OAM Graceful TPS commands on page 554
    - OAM IP Phone Loss Plan (UK) commands on page 555
    - OAM Patch and Patching Tool commands on page 556
    - OAM General Trace Tool commands on page 558
    - OAM Protocol Trace Tool commands for the Network Connection Service on page 559
    - OAM Maintenance Audit commands on page 560

- PDT security shell commands on page 561
• MC32S Command Line Interface commands on page 561
- OAM security shell commands on page 561
• Table 37: OAM CLI command groups on page 562
• Table 38: OAM General commands on page 563
• Table 39: OAM VGW commands on page 563
• Table 40: OAM iset commands on page 564
• Table 41: OAM disk commands on page 566
• Table 42: OAM special commands on page 568
• Table 43: OAM Security commands on page 569
- PDT security shell commands on page 569
Table 44: PDT CLI command groups on page 570
- PDT Command groups on page 570
• Table 45: PDT General commands on page 571
• Table 46: PDT system commands on page 572
• Table 47: PDT Debug commands on page 575
• Table 48: PDT disk commands on page 576
• Table 49: PDT special commands on page 577
• Table 50: PDT Security commands on page 579

Introduction

This chapter describes the Command Line Interface (CLI) and associated commands for each Media Card supported in an Avaya Communication Server 1000 system.

Overview

There are two types of Media Cards supported in an Avaya CS 1000 system – the ITG-SA and MC32S.

Access to a Media Card CLI is controlled by userid/password combination. Each user has a designated userid/password combination. Userid/password combinations are associated with security shells. Security shells control what commands are available in the CLI of each card. There are two types of security shells – an Operations, Administration, and Maintenance

(OAM) security shell that provides access to commands used in the operation, administration and maintenance of the Media Cards, and a Problem Determination Tool (PDT) security shell that provides access to commands used for analyzing and/or debugging any operational problems that occur on the Media Cards. If a userid/password combination is associated with the PDT security shell, the corresponding user has both OAM and PDT security shell access and capabilities.

The information in this chapter is structured in accordance with the CLI infrastructure for each Media Card. The CLI infrastructure consists of Command Groups that group together commands of similar functionality or purpose. All Command Groups and associated commands available in the OAM security shell are available in the PDT security shell by default. Some Command Groups and associated commands are only available in the PDT security shell. Each Command Group is documented in a table that contains the associated commands, a description of each command, and an indication as to whether the command is available through the General Command interface in Element Manager.

A list of Command Groups available in a security shell for a Media Card is available at the CLI command prompt for each card. A list of the commands available in a specific Command Group in a security shell is also available at the CLI command prompt for each card. In addition, help for individual commands is available at the CLI command prompt for each card.

This chapter presents information in two major sections – one section describing the CLI for the ITG-SA Media Card and the other section describing the CLI for the MC32S Media Card. Each major section contains two minor sections, one describing the Command Groups and commands available in the OAM security shell for the card(s), and the other describing the Command Groups and commands available in the PDT security shell for the card(s).

The PDT security shell sections contain tables for two categories of Command Groups – those that are only available in the PDT security shell, and those that are available in both the OAM and PDT security shells. The tables representing the second category of Command Group contain the commands that are available only in the PDT security shell. Commands that are available in the Command Groups in the OAM security shell are not repeated in the equivalent Command Groups in the PDT security shell section.

ITG-SA command line interface commands

OAM security shell commands

This section lists the Command Groups and commands available in the Operations, Administration, and Maintenance [OAM]) security shell for the ITG-SA and MC32S media cards. To access the OAM security shell of the ITG-SA media card, you must logon to the card with your userid/password combination. The OAM security shell can only be accessed if your

password is configured for OAM access. The CLI command prompt in the OAM security shell is '**ipl>**'.

The following section identifies the Command Groups in the OAM security shell. All subsequent sections are specific to a given OAM Command Group and describe the commands in the Command Group.

OAM Command groups

The following table lists the Command Groups in the OAM security shell. To display a list of the Command Groups available in the OAM security shell, type **help** at the OAM security shell prompt (*ipl*>).

Table 20: OAM CLI command groups

Command group	Description	Commands
General Purpose	General purpose commands.	Table 21: OAM General purpose commands on page 544
File Transfer	File transfer commands.	Table 22: OAM File transfer commands on page 546
IP configuration	IP configuration commands.	Table 23: OAM IP configuration commands on page 549
Reset	Reset commands.	Table 24: OAM Reset commands on page 550
DSP	DSP commands.	Table 25: OAM DSP commands on page 550
Upgrade	Upgrade commands.	Table 26: OAM IP Phone firmware upgrade commands on page 550
IPL> shell	IPL> shell command.	Table 27: OAM Shell command on page 553
Voice Gateway	Voice Gateway commands.	Table 28: OAM Voice Gateway commands on page 553
Data Path Capture Tool	Data path capture tool commands.	Table 29: OAM Data Path Capture Tool

Command group	Description	Commands
		commands on page 553
Graceful Disable	Graceful disable commands.	Table 30: OAM Graceful TPS commands on page 554
IP Phone Loss Plan	IP Phone loss plan commands.	Table 31: OAM IP Phone Loss Plan (UK) commands on page 555
Patching Tool	Patching tool commands.	Table 32: OAM Patch and Patching Tool commands on page 556
General trace tool	General trace tool commands.	Table 33: OAM General Trace Tool commands on page 558
Protocol trace tool	Protocol trace tool commands for the Network Connection Service.	Table 34: OAM Protocol Trace Tool commands for the Network Connection Service on page 559
Maintenance audit	Maintenance audit commands.	Table 35: OAM Maintenance Audit commands on page 560
Security	Intrasystem and cryptographic key support commands.	OAM Security commands on page 561

OAM Commands

The following sections contain the commands available within each Command Group in the OAM security shell. To display a list of commands in a specific OAM Command Group, type **`help <command group name>`** at the OAM security shell prompt (*ipl*>).

OAM General purpose commands

The following table lists the OAM general purpose commands in the OAM General purpose command group.

Table 21: OAM General purpose commands

Command	Description	Element Manager
`i`	Displays a summary of task control block information.	Y
`itghelp`	Displays the complete command list. ? also shows the command list.	N/A
`logout`	Exits the CLI.	N/A
`routeadd ["Host/ Network IP address"] ["IP Gateway"]`	Adds a route to the network routing table. The route is added to the host portion of the routing table.	Y
`routeshow`	Displays the current host and network routing table.	Y
`logprintoff`	Turns OFF logging for the current logged-in TTY session.	N/A
`logprinton`	Turn ON logging for the current logged-in TTY session.	N/A
`chkdsk ["disk"] [instruction]`	Checks file system consistency. Checks the internal file system for errors. Where: • ["disk"] specifies the target disk ("/C:") • [instruction] specifies the action to be performed - 1 = repair file system errors and save the damaged clusters in files. - 2 = repair file system errors and return damaged cluster to the free pool.	Y
`ping ["host"] [numPackets]`	Tests that a remote host is reachable. This command sends an ICMP ECHO_REQUEST packet to a network host. The host matching the destination address in the packet responds to the request. If a response is not returned, the sender times out. This command is useful to determine if other hosts or Voice Gateway Media Cards are communicating with the sender card. Where:	Y

Command	Description	Element Manager
	• ["host"] = the IP address of the network host to ping • [numPackets] = the number of ICMP ECHO_REQUEST packets to send If not specified, ping runs until it is stopped by Ctrl-C.	
itgcardshow	Displays Voice Gateway Media Card information.	Y
itgmemshow	Displays memory usage on the Voice Gateway Media Card.	Y
ifshow	Displays the attached network interfaces.	Y
IpInfoShow	Displays information about an IP telephony node. • IP addresses for the ELAN and TLAN subnets • default router for the ELAN and TLAN subnets • subnet mask for the ELAN and TLAN subnets • IP routing table • IP configuration of the node	Y
serialnumshow	Displays the serial number and PEC of the Voice Gateway Media Card card. This is the same serial number displayed in the LD 32 IDC command.	Y
firmwareversionshow	Displays the firmware version number.	Y
numChannelsShow	Displays number of available channels.	Y
swversionshow	Displays the software version.	Y
logFileOn	Turns on error logging to the syslog file.	N/A
logFileOff	Turns off error logging to the syslog file.	N/A
logshow	Displays information about the current logging configuration. Indicates whether logging is on or off.	Y
logconsoleon	Turns ON error logging to the console.	Y
logconsoleoff	Turns OFF error logging to the console.	N/A
pbxlinkshow	Displays the PBX link status. Displays information about the link to the CPU, including the configuration and link status.	Y

Command	Description	Element Manager
`itgalarmtest`	Generates `ITGxxxx` test alarms.	Y
`itsalarmtest`	Generates `ITSxxxx` test alarms.	N/A
`itgPLThreshold [xxx]`	Sets the packet loss logging and alarm threshold. Where: [xxx] = a number between 1 and 1000, represents the threshold in 0.1% increments. The default value is 10 (1%). Packet loss which exceeds the threshold generates an SNMP trap and writes a message to the log file if logging is enabled.	N/A
`elmshow`	Displays a list of supported languages.	N/A
`itgchanstateshow`	Displays the state for channels. e.g. busy or idle.	Y

OAM File transfer commands

The following table lists the OAM file transfer commands in the OAM File transfer command group.

Table 22: OAM File transfer commands

Command	Description	Element Manager
`swDownload ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]`	Loads a new version of software from the FTP host to the Voice Gateway Media Card. Updates the software on the Voice Gateway Media Card with the binary file received from an FTP server corresponding to the ["hostname"] IP address. The Voice Gateway Media Card FTP client performs a Get which downloads the file to the flash bank. A checksum is calculated to verify correct delivery. Once the new software version is successfully downloaded, the Voice Gateway Media Card must be rebooted with cardReset to run the new software. ["Hostname"] refers to either the IP address of the FTP host, the Voice Gateway Media Card itself, or another Voice Gateway Media Card, when a PC card in the /A: drive of the Voice Gateway Media Card contains the software binary file.	N/A
`configFileGet ["hostname"] ["username"]`	Sends an updated CONFIG.INI file from TM to the Voice Gateway Media Card.	Y

Command	Description	Element Manager
["password"] ["directory path"] ["filename"]	Updates the CONFIG.INI file on the Voice Gateway Media Card with the CONFIG.INI file on the specified host, account, and path. The configFileGet task on the ITG host initiates an FTP session with the given parameters and downloads the file to flash file system. The CONFIG.INI file also contains the NRS IP address, gateway password, and gateway DN-port mapping table.	
bootPFileGet ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]	Updates the BOOTPtab file on the Voice Gateway Media Card with the BOOTPtab file on the specified host, account and path. The bootpFileGet task on the ITG host initiates an FTP session with the given parameters and downloads the file to flash file system.	Y
hostFileGet ["hostname"] ["username"] ["password"] ["directory path"] ["filename"] ["ITGFileName"] [listener]	Transfers any file from an FTP Server to the Voice Gateway Media Card. This command gets any file from the host and does a Get using FTP to the Voice Gateway Media Card. ["ITGFileName"] = full path AND filename of where the file is to be placed. [listener] = indicates which module to inform of the successful file transfer. It can be set to –1 to be disabled.	Y
currOMFilePut ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]	Sends the current Operational Measurements (OM) file to the specified host. The OMFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the Voice Gateway Media Card Operational Measurements file to the specified location on the host.	Y
prevOMFilePut ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]	Sends the previous Operational Measurements (OM) file to the specified host. The OMFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the Voice Gateway Media Card Operational Measurements file to the specified location on the host.	Y
LogFilePut ["hostname"] ["username"]	Sends the syslog file from the Voice Gateway Media Card to TM.	N/A

Command	Description	Element Manager
["password"] ["directory path"] ["filename"]		
bootPFilePut ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]	Sends the BOOTPtab file from the Voice Gateway Media Card to TM.	Y
hostFilePut ["hostname"] ["username"] ["password"] ["directory path"] ["filename"] ["ITGFileName"]	Transfers any file from the Voice Gateway Media Card to an FTP Server.	Y
omFilePut ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]	Sends the current Operational Measurements (OM) file to the specified host.	N/A
firmwareFileGet ["ServerIP"] ["UserID"] ["Password"] ["Directory path"] ["Filename"]	Initiates a firmware download from a specified FTP server. After the download is completed, the downloaded file is checked for Enhanced Header (or proper naming). If the file is considered a valid firmware file, the UMS database is updated accordingly. Where: • ["ServerIP"] – FTP server IP address from where the firmware will be retrieved • ["UserID"], ["Password"] – credentials for logging into the FTP server • ["directory path"] – absolute or relative path to the firmware file (does not include the file name itself) • ["Filename"] – name of the firmware file on the FTP server	Y

Command	Description	Element Manager
	Use the **firmwareFileGet** command instead of the **firmwareFileGetI2004, firmwareFileGetI2002,** and **firmwareFileGetIPP2** commands.	
firmwareFilePut ["ServerIP"] ["UserID"] ["Password"] ["Directory path"] ["Filename"]	Uploads F/W file to the specified FTP server. The file is added for consistency with existing firmwareFilePutI2004 and firmwareFilePutI2002 commands.	

OAM IP configuration commands

The following table lists the OAM IP configuration commands in the OAM IP configuration command group.

Table 23: OAM IP configuration commands

Command	Description	Element Manager
NVRIPSet	Sets the IP address in NVRAM.	N/A
NVRGWSet	Sets the default gateway address in NVRAM.	N/A
NVRSMSet	Sets the subnet mask in NVRAM.	N/A
NVRIPShow	Displays the values of the IP parameters that reside in NVRAM.	N/A
NVRClear	Clears the IP parameters in NVRAM.	N/A
nvramLeaderSet	Sets the leader bit in NVRAM.	N/A
nvramLeaderClr	Clears the leader bit in NVRAM, but does not erase the IP parameters in NVRAM.	N/A
setLeader [IP Address] [IP gateway] [subnet mask]	Sets the IP address, gateway, subnet mask. Also sets the boot method to static, and the Leader bit in NVRAM. This command performs all of the necessary actions to make a Leader.	Y
clearLeader	Clears the Leader information in NVRAM, sets the boot method to use BOOTP, and removes the old configuration files. Makes a Leader card into a Follower card.	Y
tLanDuplexSet	Sets the duplex mode of the TLAN network interface.	N/A

Command	Description	Element Manager
tLanSpeedSet	Sets the speed of the TLAN network interface.	N/A

OAM Reset commands

The following table lists the OAM reset commands in the OAM Reset command group.

Table 24: OAM Reset commands

Command	Description	Element Manager
cardreset	Resets the Voice Gateway Media Card card. Performs a warm reboot of card.	N/A
resetOM	Resets the timer for the operational measurement file.	Y
lastResetReason	Displays the reason for the last card reset.	N/A

OAM DSP commands

The following table lists the OAM DSP commands in the OAM DSP Command Group.

Table 25: OAM DSP commands

Command	Description	Element Manager
DSPReset	Resets the specified DSP.	N/A
DSPNumShow	Displays the number of DSP channels for each DSP DB.	Y
dspSWVersionShow		N/A

OAM IP Phone firmware upgrade commands

The following table lists the OAM IP Phone firmware upgrade commands in the OAM SIP Phone firmware upgrade Command Group.

Table 26: OAM IP Phone firmware upgrade commands

Command	Description	Element Manager
shellPasswordSet	Changes the current user name and password of the OAM security shell.	N/A
umsUpgradeAll ["hh:mmx"]	Upgrades all registered sets according to policy and firmware file. Where:	Y

Command	Description	Element Manager
	• hh:mm = specifies the time when the upgrade will occur • x = specifies whether the time is AM or PM - a = AM - p = PM **Caution:** If the umsUpgradeAll command is used without the time parameter, all IP Phones registered on cards that are logged into are immediately taken out of service. Use the time parameter with the command to prevent this from happening.	
`umsUpgradeTimerShow`	Displays the upgrade schedule.	Y
`umsUpgradeTimerCancel`	Cancels the scheduled upgrade.	Y
`firmwareFileGet ["ServerIP"] ["UserID"] ["Password"] ["Directory path"] ["Filename"]`	Initiates a firmware download from a specified FTP server. After the download is completed, the downloaded file is checked for Enhanced Header (or proper naming). If the file is considered a valid firmware file, the UMS database is updated accordingly. Where: • ["ServerIP"] – FTP server IP address from where the firmware will be retrieved • ["UserID"], ["Password"] – credentials for logging into the FTP server • ["directory path"] – absolute or relative path to the firmware file (does not include the file name itself) • ["Filename"] – name of the firmware file on the FTP server Use the **`firmwareFileGet`** command instead of the **`firmwareFileGetI2004`**, **`firmwareFileGetI2002`**, and **`firmwareFileGetIPP2`** commands.	Y
`firmwareFilePut ["ServerIP"] ["UserID"] ["Password"]`	Uploads F/W file to the specified FTP server. The file is added for consistency with existing firmwareFilePutI2004 and firmwareFilePutI2002 commands.	

Command	Description	Element Manager
["Directory path"] ["Filename"]		
uftpTurboMode ["HH:MM/start/stop/on/off"] [MM] ["show"]	Configures maintenance mode. Where: • "HH:MM" – time to enter Maintenance Mode in 24-hour format • "start" – enter Maintenance Mode immediately • "stop" – stop Maintenance Mode • "on" – allow Signaling Server to enter Maintenance Mode • "off" – do not allow Signaling Server to enter Maintenance Mode • MM – optional parameter that defines the length of time in minutes that Maintenance Mode is to be maintained • "show" – displays the same output as uftpTurboModeShow If no parameter is entered, Upgrade Manager defaults to uftpturboMode "start".	Y
uftpTurboModeShow	Displays the current status of maintenance mode.	Y
uftpTurboModeTimeoutSet [MM]	Configures the idle timeout timer for maintenance mode. Where: MM – optional parameter that defines the number of minutes the Upgrade Manager waits after the last firmware download job is started before returning the Signaling Server to normal mode If this parameter is configured as 0 (zero), the Upgrade Manager never exits Maintenance Mode unless the umsUpgradeModeSet command is issued with the "stop" parameter. If no parameter is entered, then the current timeout setting is displayed.	Y

OAM Shell command

The following table lists the OAM shell command in the OAM Shell Command Group.

Table 27: OAM Shell command

Command	Description	Element Manager
shellPasswordSet	Changes the current user name and password of the OAM security shell.	N/A

OAM Voice Gateway commands

The following table lists the OAM shell command in the OAM Shell Command Group.

Table 28: OAM Voice Gateway commands

Command	Description	Element Manager
disiVGW	Gracefully disables Voice Gateway services.	N/A
enaVGW	Enables the Voice Gateway service.	N/A
vgwPLLog	Toggle gateway packet loss logging ON/OFF.	N/A
vgwshow	Displays information about the active (non-idle and equipped) gateway channels. Entering this command with the IP Address of an IP Phone displays the identification of the Voice Gateway Media Card that has the gateway channel being used by the IP Phone. This is useful when there is a requirement to collect gateway statistics (for example, packet loss).	Y
vgwShowALL	Displays information about all gateway channels.	Y
PrintVGWChannels		
ipstatShow		
cardRoleShow		

OAM Data Path Capture Tool commands

The following table lists the OAM data path capture tool commands in the OAM Data Path Capture Tool Command Group.

Table 29: OAM Data Path Capture Tool commands

Command	Description	Element Manager
captureStart [tcid]	Begins the audio data capture operation for a specified gateway channel. Where [tcid] = gateway channel id.	N/A

Command	Description	Element Manager
	• 0 to 23 for ITG-P card • 0 to 31 for MC32 card Audio data on the gateway channel begins to be captured to the circular queue.	
`captureStop`	Stops the audio data capture.	N/A
`captureSaveLocal ["filename"]`	Dumps the contents of the circular queue (captured gateway channel audio data) to the specified file on the memory PC Card inserted in the /A: drive on the Voice Gateway Media Card faceplate. Where ["filename"] = the name to assign to the captured gateway channel audio data file on the memory PC card.	N/A
`captureSaveRemote ["filename"]`	FTPs the contents of the circular queue (captured gateway channel audio data) to the specified file on the remove server. Where ["filename"] = the name to assign to the captured gateway channel audio data file on the FTP server.	N/A
`captureFree`	Frees the circular queue from gateway channel audio data capture operations.	N/A

OAM Graceful TPS commands

The following table lists the OAM graceful TPS commands in the OAM Graceful TPS Command Group.

Table 30: OAM Graceful TPS commands

Command	Description	Element Manager
`disServices`	Gracefully switches all registered resources (IP Phones, Virtual Trunks, and Voice Gateways) to the other Voice Gateway Media Cards or Signaling Servers located in the same node. This command does not interrupt established calls.	Y
`disiAll`	Gracefully voice gateway service on the Voice Gateway Media Card.	Y
`disiTPS`	Gracefully disables the LTPS service on the Voice Gateway Media Card.	Y

Command	Description	Element Manager
	Prevents new IP Phones from registering on the card, and all registered IP Phones are redirected to another card, when idle.	
disiVGW	Gracefully disables Voice Gateway services.	N/A
enaALL	Enables voice gateway service on the Voice Gateway Media Card.	Y
enlServices	Enables all Voice Gateway Media Cards and Signaling Servers in the node to accept registration of resources.	Y
enaTPS	Enables TPS service (opposite of disitps)	Y
enaVGW	Enables the Voice Gateway service.	N/A

OAM IP Phone Loss Plan (UK) commands

The following table lists the OAM IP Phone loss plan (UK) command in the OAM IP Phone Loss Plan (UK) Command Group.

Table 31: OAM IP Phone Loss Plan (UK) commands

Command	Description	Element Manager
UKLossPlanSet	Sets the loss plan values on the IP Phone to UK-specific values.	Y
UKLossPlanClr	Sets the loss plan values on the IP Phone to default values.	Y
lossPlanPrt	Displays the current IP Phone loss plan settings. Displays the offsets and current values for the handset, headset, and handsfree RLR and SLR.	Y
lossPlanSet [transducer] [rlrOffset] [slrOffset]	Allows a variable offset from the default loss plan to be entered for the specified transducer (handset, headset, or handsfree). Where: • [transducer] = identity of the transducer • [rlrOffset] = value to offset the audio level heard on the IP Phone Positive numbers reduce the audio level (add loss), and negative numbers increase the audio level (add gain). • [slrOffset] = value to offset the audio level transmitted from the IP Phone	Y

Command	Description	Element Manager
	Positive numbers reduce the audio level (add loss), and negative numbers increase the audio level (add gain).	
lossPlanClr	Sets the loss plan values on the IP Phone to default values. Removes the loss plan adjustments and returs the IP Phone to the default loss plan levels.	N/A

OAM Patch and Patching Tool commands

The following table lists the OAM patch and patching tool commands in the OAM Patch and Patching Tool Command Group.

Table 32: OAM Patch and Patching Tool commands

Command	Description	Element Manager
pload ["patch-filename"]	Loads a patch file from the file system in Flash memory into DRAM memory, where [patch-filename] is the filename or path of the patch file. If a filename alone is provided, the patch must be in the /C:/u/patch directory. Otherwise, the full or relative path can be provided. When a patch is successfully loaded, the command returns a patch handle number. The patch handle number is used as input to other patch commands (pins, poos, pout, and plis). The loaded patch is inactive until it is put into service using the pins command. If the command is issued without a parameter, you are prompted for the patch filename and other information.	N/A
pins [handle]	Puts a patch that has been loaded into memory (using the pload command) into service, where [handle] is the number returned by the pload command. If the command is issued without a parameter, you are prompted to enter a [handle]. If issued successfully, the command indicates the global procedures, functions, or areas of memory affected by the patch. You are then prompted and have the choice to proceed or not to proceed.	N/A
poos [handle]	Deactivates a patch (takes it out-of-service) by restoring the patched procedure to its original state.	N/A

Command	Description	Element Manager
	If the poos command is issued without a parameter, you are prompted to enter a [handle].	
`pout [handle]`	Removes a patch from DRAM memory. The patch must be taken out-of-service (using the poos command) before it can be removed from the system. If the pout command is issued without a parameter, you are prompted to enter a handle.	N/A
`pstat [handle]`	Displays summary status information for one or all loaded patches. For each patch, the following information is displayed: patch handle, filename, reference number, whether the patch is in-service or out-of-service, the reason why the patch is out-of-service (if applicable), and whether the patch is marked for retention or not. Patch retention means that if a reset occurs, then the patch is automatically reloaded into memory and its state (active or inactive) is restored to what it was prior to the system going down. If the [handle] is provided, only the information for the specified patch is displayed. If the command is issued without a parameter, information for all the patches is displayed.	N/A
`plis [handle]`	Lists detailed patch status information for a loaded patch. If the command is issued without a parameter, you are prompted to enter a [handle].	N/A
`pnew`	Creates memory patches for the Media Gateway Card. The command has no parameter(s). The release of the patch is assumed to be the same as that of the current load. The address to be patched is checked to ensure that it is in range. For each address that is changed, the "old" contents are assumed to be the current contents of that memory address. If a path is not provided for the new path filename then it is assumed that the patch is in the /C:/u/ patch directory. Once a memory patch is created using the pnew command, it can be loaded and activated like any other patch.	N/A

OAM General Trace Tool commands

The following table lists the OAM general trace tool commands in the OAM General Trace Tool Command Group.

Table 33: OAM General Trace Tool commands

Command	Description	Element Manager
`traceShow`	Displays the names of active traces in the system.	Y
`traceAllOff`	Disables the trace facilities from writing to the TTY, SYSLOG, and specified files. Causes all traces that use the monitorLib server to stop their output. This is a temporary disabling function.	Y
`tracePrintOff`	Disables the trace facilities from writing to the TTY. Blocks all logging of information received by the monitorLib service to the TTY output. This does not include traces directed through the monitorLib service to the RPT.LOG or SYSLOG.n services.	Y
`traceFileOff`	Disables the trace facilities from writing to the SYSLOG and specified files. Causes the monitorLib server to stop logging to the log files any and all trace information received by the service. The log files include syslog.n for the Voice Gateway Media Card and rpt.log for the Signaling Server.	Y
`traceAllOn`	Enables the trace facilities to resume writing to the TTY, SYSLOG, and/or specified files. Clears the blocking of all trace information imposed on the monitorLib service by the traceAllOff, tracePrintOff, and traceFileOff commands. By default, all tracing is on.	Y
`tracePrintOn`	Enables the trace facilities to resume writing to the TTY. Clears only the TTY output blocking that was imposed by the traceAllOff and tracePrintOff commands.	Y
`traceFileOn`	Enables the trace facilities to resume writing to the SYSLOG and/or specified files. Clears only the blocking of logging to files that was imposed by the traceAllOff and traceFileOff commands.	Y

OAM Protocol Trace Tool commands for the Network Connection Service

The following table lists the OAM protocol trace tool commands for the Network Connection Service (NCS) in the OAM Protocol Trace Tool commands for the Network Connection Service Command Group.

Table 34: OAM Protocol Trace Tool commands for the Network Connection Service

Command	Description	Element Manager
`tpsARTrace IP [IP address] ID [User ID] ALL`	Enables tracing for the Network Connection Server (NCS). Allows tracing of the tpsAR protocol, which is used to determine where an IP Phone should register. Where: • IP address = a string containing the IP Phone's IP address • User ID = the ID of the IP Phone to be traced (the DN used to log in) or the H323_Alias of where the IP Phone is trying to register • ALL = all IP Phones are to be monitored	Y
`tpsARTraceOff IP [IP address] ID [User ID] ALL`	Disables tracing for the Network Connection Server (NCS). Removes the specified endpoint from the list of endpoints to be traced. Where: • IP address = a string containing the IP Phone's IP address • User ID = the ID of the IP Phone being traced (the DN used to log in) or the H323_Alias of where the IP Phone is =registered • ALL = removes monitoring of all IP Phones	N/A
`tpsAROutput [Output_Destination] ["File Pathname"]`	Modifies the destination for the traced output of the NCS. Sets the output for all tpsAR protocol traces. • [Output_Destination] = where all the trace messages for the tpsARTraceSet are to be directed The values are: - 1 = TTY - 2 = RPTLOG - 3 = File - 4 =TTY + File	N/A

Command	Description	Element Manager
	If the command is run from the OAM prompt or PDT prompt on the Signaling Server, then the values are the actual word, not a number: - TTY - RPTLOG - FILE - TTY + FILE • ["File Pathname"] = specifies the output file name if option 3 or 4 is selected.	
`tpsARTraceSettings`	Displays the trace settings and items being traced for the NCS trace. Displays the trace tool settings, which endpoints are being traced, and where the trace output is being directed.	N/A
`tpsARTraceHelp`	Displays help on the tpsARTrace commands. Displays a list of all CLI commands used for tracing tpsAR protocol messages, including usage and parameters.	N/A

OAM Maintenance Audit commands

The following table lists the OAM maintenance audit command in the OAM Maintenance Audit Command Group.

Table 35: OAM Maintenance Audit commands

Command	Description	Element Manager
`auditShow`	Displays the following information about a Voice Gateway Media Card: • whether a card reboot is enabled • the time a card reboot will occur if a non- critical task is found suspended • a list of all tasks being monitored, and their designation (critical or non-critical)	N/A
`auditHistoryShow`	Displays the recent history of the audit task activity in the audit.his file.	N/A
`auditRebootSet [switch]`	Globally disables the card reboot from this audit task. Where [switch] specifies whether a card reboot should occur when a suspended task is detected.	N/A

Command	Description	Element Manager
	This switch is set to "1" by default (reboot occurs). If set to "0", no card reboot occurs when a suspended task is found for critical or non-critical tasks.	
`auditRebootTimeSet ["HH:MM"]`	Sets the reset time for non-critical suspended tasks. Where: ["HH:MM"] = the reset time. Format is 24-hour clock. Default is 02:00 (2 AM)	N/A

OAM Security commands

The following table lists the OAM security commands in the OAM Security Command Group.

Table 36: OAM Security commands

Command	Description	Element Manager
`statSecDomain`	Show the Primary Security Server IP address and fingerprint.	N/A

PDT security shell commands

New PDT security command group containing new commands in support of the Secure Transport enhancement.

- joinSecDomain
- leaveSecDomain

MC32S Command Line Interface commands

OAM security shell commands

This section lists the Command Groups and commands available in the Operations, Administration, and Maintenance [OAM]) security shell for the MC32S Voice Gateway Media Card. To access the OAM security shell, you must force the MC32S logon prompt to appear by holding down the CTRL key and typing **oam**, and logon to the card with your userid/password

combination. The OAM security shell can only be accessed if your password is configured for OAM access. The CLI command prompt in the OAM security shell is **<oam>**.

The following section identifies the Command Groups in the OAM security shell. All subsequent sections are specific to a given OAM Command Group and describe the commands in the Command Group.

OAM Command groups

The following table lists the Command Groups in the OAM security shell. To display a list of the Command Groups available in the OAM security shell, type **help** at the OAM security shell prompt (*oam*>).

Table 37: OAM CLI command groups

Command group	Description	Commands
General	General purpose commands.	Table 38: OAM General commands on page 563
VGW	Voice Gateway application administration and maintenance commands.	Table 39: OAM VGW commands on page 563
ISET	IP Phone and LTPS administration and maintenance commands.	Table 40: OAM iset commands on page 564
Disk	Disk and file commands.	Table 41: OAM disk commands on page 566
Special	Special purpose PDT commands.	Table 42: OAM special commands on page 568
Security	Intrasystem and cryptographic key support commands.	Table 43: OAM Security commands on page 569

OAM Commands

The following sections contain the commands available within each Command Group in the OAM security shell. To display a list of commands in a specific OAM Command Group, type **help <command group name>** at the OAM security shell prompt (*oam*>).

OAM General commands: general purpose

The following table lists the OAM general purpose commands in the OAM General command group.

Table 38: OAM General commands

Command	Description	Element Manager
`exit`	Terminate current shell.	N/A
`help`	Show a list of available commands.	N/A
`version`	Displays vxWorks™ version, date of build, and other information.	Y
`ifshow`	Displays the attached network interfaces.	Y
`ping ["host"] [numPackets]`	Tests that a remote host is reachable. This command sends an ICMP ECHO_REQUEST packet to a network host. The host matching the destination address in the packet responds to the request. If a response is not returned, the sender times out. This command is useful to determine if other hosts or Voice Gateway Media Cards are communicating with the sender card. Where: • ["host"] = the IP address of the network host to ping • [numPackets] = the number of ICMP ECHO_REQUEST packets to send If not specified, ping runs until it is stopped by Ctrl-C.	Y

OAM VGW commands: MC32S gateway application administration and maintenance

The following table lists the OAM voice gateway application administration and maintenance commands in the OAM VGW command group.

Table 39: OAM VGW commands

Command	Description	Element Manager
`dspnumshow`	Displays the number of DSP channels for each DSP DB.	Y
`dspchanstateshow`	Displays the state of all channels on the DSP DBs.	Y

Command	Description	Element Manager
dsphwcheck	Perform a basic DSP hardware diagnostic check.	Y
dsplooptest [card1] [channel1] [card2] [channel2]	Perform a DSP loopback test for all currently inactive channels or given channels.	Y
vgwshow	Displays information about the active (non-idle and equipped) gateway channels. Entering this command with the IP Address of an IP Phone displays the identification of the Voice Gateway Media Card that has the gateway channel being used by the IP Phone. This is useful when there is a requirement to collect gateway statistics (for example, packet loss).	Y
vgwshowall	Displays information about all gateway channels.	Y
vgwshowcard	Displays all channel information for a specified card.	Y
dspreset	Reset DSPs.	N/A
vgwpllog	Toggle gateway packet loss logging ON/OFF.	N/A
numchannelsshow	Displays number of available channels.	Y
ommshow	Displays the current OM data on the console.	Y
resetom	Resets the timer for the operational measurement file.	Y
itgchanstateshow	Displays the state for channels. e.g. busy or idle.	Y

OAM iset commands: iset module

The following table lists the OAM iset module commands in the OAM iset command group.

Table 40: OAM iset commands

Command	Description	Element Manager
elmshow	Displays a list of supported languages.	N/A
disitps	Gracefully disables the LTPS service on the Voice Gateway Media Card.	N/A

Command	Description	Element Manager
	Prevents new IP Phones from registering on the card, and all registered IP Phones are redirected to another card, when idle.	
`enatps`	Enables TPS service (opposite of `disitps`)	N/A
`uklossplanset`	Sets the loss plan values on the IP Phone to UK-specific values.	N/A
`lossplanset [transducer] [rlrOffset] [slrOffset]`	Allows a variable offset from the default loss plan to be entered for the specified transducer (handset, headset, or handsfree). Where: • [transducer] = identity of the transducer • [rlrOffset] = value to offset the audio level heard on the IP Phone Positive numbers reduce the audio level (add loss), and negative numbers increase the audio level (add gain). • [slrOffset] = value to offset the audio level transmitted from the IP Phone Positive numbers reduce the audio level (add loss), and negative numbers increase the audio level (add gain).	N/A
`uklossplanclr`	Sets the loss plan values on the IP Phone to default values.	N/A
`lossplanclr`	Sets the loss plan values on the IP Phone to default values. Removes the loss plan adjustments and returs the IP Phone to the default loss plan levels.	N/A
`lossplanprt`	Displays the current IP Phone loss plan settings. Displays the offsets and current values for the handset, headset, and handsfree RLR and SLR.	N/A
`uftpshow`	Displays IP Phone firmware download information.	N/A
`itgplthreshold [xxx]`	Sets the packet loss logging and alarm threshold. Where: [xxx] = a number between 1 and 1000, represents the threshold in 0.1% increments.	N/A

Command	Description	Element Manager
	The default value is 10 (1%). Packet loss which exceeds the threshold generates an SNMP trap and writes a message to the log file if logging is enabled.	
disservices	Gracefully switches all registered resources (IP Phones, Virtual Trunks, and Voice Gateways) to the other Voice Gateway Media Cards or Signaling Servers located in the same node. This command does not interrupt established calls.	Y
enlservices	Causes all the Voice Gateway Media Cards and Signaling Servers in the node to accept registration of resources.	Y
servicestatusshow	Displays the status of services (tps/iset/vtrk/gk).	Y

OAM disk commands: disk and file commands

The following table lists the OAM disk and file commands in the OAM disk command group.

Table 41: OAM disk commands

Command	Description	Element Manager
bootpfileget ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]	Updates the BOOTPtab file on the Voice Gateway Media Card with the BOOTPtab file on the specified host, account and path. The bootpFileGet task on the host initiates an FTP session with the given parameters and downloads the file to the flash file system.	N/A
bootpfileput ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]	Sends the BOOTPtab file from the Voice Gateway Media Card to TM.	N/A
configfileget ["hostname"] ["username"] ["password"] ["directory	Sends an updated CONFIG.INI file from TM to the Voice Gateway Media Card. Updates the CONFIG.INI file on the Voice Gateway Media Card with the CONFIG.INI file on the specified host, account, and path. The	N/A

Command	Description	Element Manager
path"] ["filename"]	configFileGet task on the ITG host initiates an FTP session with the given parameters and downloads the file to flash file system. The CONFIG.INI file also contains the NRS IP address, gateway password, and gateway DN-port mapping table.	
curromfileput ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]	Sends the current Operational Measurements (OM) file to the specified host. The OMFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the Voice Gateway Media Card Operational Measurements file to the specified location on the host.	N/A
hostfileget ["hostname"] ["username"] ["password"] ["directory path"] ["filename"] ["ITGFileName"] [listener]	Transfers any file from an FTP Server to the Voice Gateway Media Card. This command gets any file from the host and does a Get using FTP to the Voice Gateway Media Card. ["ITGFileName"] = full path AND filename of where the file is to be placed. [listener] = indicates which module to inform of the successful file transfer. It can be set to –1 to disable feature.	N/A
hostfileput ["hostname"] ["username"] ["password"] ["directory path"] ["filename"] ["ITGFileName"]	Transfers any file from the Voice Gateway Media Card to an FTP Server.	N/A
omfileput ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]	Sends the current Operational Measurements (OM) file to the specified host.	N/A
prevomfileput ["hostname"] ["username"] ["password"] ["directory	Sends the previous Operational Measurements (OM) file to the specified host. The OMFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the Voice Gateway Media Card	N/A

Command	Description	Element Manager
path"] ["filename"]	Operational Measurements file to the specified location on the host.	

OAM special commands: special purpose PDT commands

The following table lists the OAM special commands in the OAM special command group.

Table 42: OAM special commands

Command	Description	Element Manager
mdp	Manipulate the DEPLIST.	N/A
testalarm	Tests SNMP traps.	Y
rdhelp	Lists all report display commands.	N/A
rdopen [filename]	Opens a report log file. Where [filename] is the name of the report file to be opened.	Y
rdgo [N]	Goes to a specific record. Where [N] is the absolute record number.	Y
rd [S] [R]	Displays a specified number of records starting at a specified point. Where: • [S] is the number of steps to traverse to the starting point. • [R] is the number of records to display. Both [S] and [R] can be negative.	Y
rds [S] [R]	Displays a specified number of records, with a symbolic dump, starting at a specified point. Where: • [S] is the number of steps to traverse to the starting point. • [R] is the number of records to display. Both [S] and [R] can be negative.	Y
rdshow	Displays general information about the current log file and the current rd settings.	Y
rdall	Displays all records.	N/A
rdtail [N]	Displays the specified number of newest records. Where [N] is the number of records to display.	Y

Command	Description	Element Manager
rdhead [N]	Displays the specified number of oldest records. Where [N] is the number of records to display.	Y
rdnext	Opens the next log file.	Y
rdprev	Opens the previous log file.	Y
rdsconvert [filename]	Converts a log file to text. Where [filename] is the name of the log file to be converted.	Y

OAM Security commands: Intrasystem and cryptographic key support

The following table lists the OAM Security commands in the OAM Security command group.

Table 43: OAM Security commands

Command	Description	Element Manager
disSecureShells	Disable all secure shells in the system.	Y
disInsecureShells	Disables all insecure shells in the system.	Y
enlInsecureShells	Enable all insecure shells in the system.	Y
enlSecureShells	Enables all secure shells in the system.	Y
isssDecom	Clean up ISSS settings and delete ISSS configuration files.	N/A
isssReset	Reset ISSS configuration.	N/A
isssShow	Print out ISSS settings.	N/A
joinSecDomain	Establish mutual trust with the primary security server.	N/A
leaveSecDomain	Remove the primary security server mutual trust information from the device.	N/A
statInsecureShells	Displays whether insecure shell access is enabled or disabled.	Y
statSecDomain	Show the Primary Security Server IP address and fingerprint.	N/A
statSecureShells	Displays whether secure shell access is enabled or disabled.	Y

PDT security shell commands

This section lists the Command Groups and commands available in the Problem Determination Tool (PDT) security shell for the MC32S Media Card. To access the PDT security shell, you

must force the MC32S Media Card logon prompt to appear by holding down the CTRL key and typing **pdt**, and logon to the card with your userid/password combination. The PDT security shell can only be accessed if your password is configured for PDT security shell access. The CLI command prompt in the PDT security shell is **'pdt>'**.

This section contains tables corresponding to Command Groups that are available in the PDT security shell. PDT security shell capabilities are inclusive of all OAM security shell capabilities. All Command Groups and commands available in the OAM security shell for the MC32S Media Card are available in the PDT security shell by default.

This section contains tables for two categories of Command Groups – those that are only available in the PDT security shell, and those that are available in both the OAM and PDT security shells, but contain commands that are only available in the PDT security shell. The tables representing the second category of Command Group contain only the commands available in the PDT security shell. Commands that are available in both security shells are not repeated in this section. See OAM security shell commands on page 561 for descriptions of these commands.

PDT Command groups

The following table lists the Command Groups that are available only in the PDT security shell (in italics), and OAM Command Groups that contain commands available only in the PDT security shell. To display a list of commands in a specific Command Group, type **help <command group name>** at the PDT security shell prompt (*pdt>*).

Table 44: PDT CLI command groups

Command group	Description	PDT Commands
General	General purpose commands.	Table 45: PDT General commands on page 571
System	MC32S platform administration and maintenance commands.	Table 46: PDT system commands on page 572
Debug	PDT debug commands.	Table 47: PDT Debug commands on page 575
disk	Disk and file commands.	Table 48: PDT disk commands on page 576
special	Special purpose PDT commands.	Table 49: PDT special commands on page 577

Command group	Description	PDT Commands
security	Intrasystem and cryptographic key support commands.	Table 50: PDT Security commands on page 579

PDT Commands

The following tables list the PDT commands in each Command Group in the PDT security shell. To display a list of commands in a specific PDT security shell Command Group, type **`help <command group name>`** at the PDT security shell prompt(*pdt*>) .

PDT General commands: general purpose

The following table lists the PDT general purpose commands in the PDT General command group. These commands are in addition to the OAM commands listed in OAM General commands: general purpose on page 563.

Table 45: PDT General commands

Command	Description	Element Manager
`devs`	Displays the list of devices.	N/A
`echo`	Echo the inputs.	N/A
`h`	Displays the 20 most recent commands entered in the shell.	N/A
`hosts`	Displays a list of hosts.	Y
`i`	Displays a summary of task control block information.	N/A
`mem`	Displays memory usage and a list of free blocks.	N/A
`rdaccess`	Displays shell access attempts.	N/A
`rx`	Receive a file over a serial connection using XMODEM.	N/A
`ti [name | taskid]`	Displays detailed task control block information. Where: • [name] is the name of the task. • [taskID] is the ID of the task. [name] and [taskID] are mutually exclusive.	N/A

PDT system commands: MC32S platform administration and maintenance

The following table lists the PDT MC32S platform administration and maintenance commands in the PDT system command group.

Table 46: PDT system commands

Command	Description	Element Manager
`mgcInfoShow`	Displays basic setup information.	Y
`mc32sinfoshow`	Displays basic information about the MC32S.	Y
`macshow`	Displays all of the MAC addresses associated with the Ethernet ports (both internal and external) on the embedded Ethernet switch.	Y
`diskshow`	Displays the total, used and available disk space available on the internal compact flash card.	Y
`memshow`	Displays the total, used and available RAM memory.	Y
`diskformat`	Formats the internal compact flash.	N/A
`ethportshow`	Displays the Ethernet port settings for the external and internal interfaces, including autonegotiation settings, duplex, port speed and port mirroring status.	N/A
`ethportmirror [port1] [port2]`	Allows mirroring of one of the embedded Ethernet switch ports. To disable mirroring of a port, use ‘none’ for port2.	N/A
`ethportdisable [port]`	Disables a port so it can be used for mirroring.	N/A
`ethportreset`	Clears all port mirroring and reenables standard embedded Etherenet switch functionality.	N/A
`ethspeedshow`	Displays the port speed and duplex setting for the ports of the embedded Ethernet switch.	Y
`dbhwshow`	Displays the model and revision numbers for installed DBs.	Y
`cardreset`	Resets the Voice Gateway Media Card card. Performs a warm reboot of card.	Y
`ipinfoshow`	Displays information about an IP telephony node. • IP addresses for the ELAN and TLAN subnets • default router for the ELAN and TLAN subnets • subnet mask for the ELAN and TLAN subnets • IP routing table • IP configuration of the node	Y

Command	Description	Element Manager
logconsoleon	Turns ON logging to the console.	Y
logconsoleoff	Turns OFF logging to the console.	N/A
logout	Exits the shell.	N/A
logprintoff	Turns OFF logging to the logged-in TTY session.	N/A
logprinton	Turn ON logging to the logged-in TTY session.	N/A
logshow	Displays information about the current logging configuration.	Y
mgcDbShow	Display information about DSP DB	Y
pbxlinkshow	Displays the PBX link status. Displays information about the link to the CPU, including the configuration and link status.	Y
routeadd ["Host/ Network IP address"] ["IP Gateway"]	Adds a route to the network routing table. The route is added to the host portion of the routing table.	Y
routeshow	Displays the current host and network routing table.	Y
serialnumshow	Displays the serial number and PEC of the card.	Y
swversionshow	Displays the software version.	Y
tlanduplexset	Sets the duplex mode of the TLAN network interface.	N/A
tlanspeedset	Sets the speed of the TLAN network interface.	N/A
mc32ssetup	Configures all IP parameters. Menu driven interface to change networking parameters.	N/A
rmonstatshow [port]	Displays the RMON statistics collected by the embedded Ethernet switch for a given port.	Y
rmonstatshowall	Displays the RMON statistics collected by the embedded Ethernet switch for all ports.	Y
rmonstatreset [port]	Resets all RMON statistics counters on the embedded Ethernet switch for a given port.	Y
rmonstatresetall	Resets all RMON statistics counters for all ports on the embedded Ethernet switch.	Y

Command	Description	Element Manager
`setleader [IP Address] [IP gateway] [subnet mask]`	Sets the IP address, gateway, subnet mask. Also sets the boot method to static, and the Leader bit in NVRAM.	Y
`clearleader`	Clears the Leader information in NVRAM, and sets the boot method to use BOOTP, thus, making the card a Follower.	Y
`swDownload ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]`	Loads a new version of software from the FTP host to the Voice Gateway Media Card. Updates the software on the Voice Gateway Media Card with the binary file received from an FTP server corresponding to the ["hostname"] IP address. The Voice Gateway Media Card FTP client performs a Get which downloads the file to the flash bank. A checksum is calculated to verify correct delivery. Once the new software version is successfully downloaded, the Voice Gateway Media Card must be rebooted with cardReset to run the new software. ["Hostname"] refers to either the IP address of the FTP host, the Voice Gateway Media Card itself, or another Voice Gateway Media Card, when a PC card in the /A: drive of the Voice Gateway Media Card contains the software binary file.	Y
`disiall`	Gracefully disables voice gateway service on the Voice Gateway Media Card.	Y
`enaall`	Enables voice gateway service on the Voice Gateway Media Card.	Y
`firmwareversionshow`	Displays the firmware version number.	Y
`itgalarmtest`	Generates `ITGxxxx` test alarms.	Y
`itgcardshow`	Displays Voice Gateway Media Card information.	Y
`itgmemshow`	Displays memory usage on the Voice Gateway Media Card.	Y
`nvramleaderclr`	Clears the leader bit in NVRAM, but does not erase the IP parameters in NVRAM.	N/A
`nvramleaderset`	Sets the leader bit in NVRAM.	N/A
`nvrclear`	Clears the IP parameters in NVRAM.	N/A
`nvripset`	Sets the IP address in NVRAM.	N/A

Command	Description	Element Manager
nvripshow	Displays the values of the IP parameters that reside in NVRAM.	N/A
nvrgwset	Sets the default gateway address in NVRAM.	N/A
nvrsmset	Sets the subnet mask in NVRAM.	N/A
displayshow	Displays the faceplate message.	Y
mspversionshow	Displays the MSP device type, ARM code, voice DSP revision, and T.38 version.	Y

PDT Debug commands: PDT debug

The following table lists the PDT debug commands in the PDT Debug command group.

Table 47: PDT Debug commands

Command	Description	Element Manager
cd [path]	Changes the default directory. Where: [path] = the path and name of the new directory. The [path] of the new directory can be specified as a relative path.	N/A
chkdsk ["disk"] [instruction]	Checks file system consistency. Checks the internal file system for errors. Where: • ["disk"] specifies the target disk ("/C:") • [instruction] specifies the action to be performed - 1 = repair file system errors and save the damaged clusters in files. - 2 = repair file system errors and return damaged cluster to the free pool.	N/A
cp	Copy many files to another directory.	N/A
copy	Copy from [input] file to [output] file.	N/A
label	Creates, changes, and/or displays a device label.	N/A
ll	Displays a long list of the contents of a directory.	N/A
ls	Displays a short list of the contents of a directory.	N/A

Command	Description	Element Manager
pwd	Displays the current (working) directory.	N/A
type	Displays the contents of a file.	N/A

PDT disk commands: disk and file commands

The following table lists the PDT disk and file commands in the PDT disk command group. These commands are in addition to the OAM commands listed in OAM disk commands: disk and file commands on page 566

Table 48: PDT disk commands

Command	Description	Element Manager
cp	Copies many files to another directory.	N/A
copy [input] [output]	Copies from one file to another file until an end-of-file (CTRL+d) is reached. Where: • [input] = the name of the file to be copied from. If NULL, stdin is used. • [output] is the name of the new or destination file to be copied to. If NULL, stdout is used.	N/A
label	Creates, changes, and/or displays a device label.	N/A
ll [path]	Displays a long list of the contents of a directory. Where: [path] = the path name of the directory. If path is not specified, the contents of the current directory are displayed.	N/A
ls [path]	Displays the contents of a directory. Where: [path] = the path name of the directory. If [path] is not specified, the contents of the current directory are displayed.	N/A
pwd	Displays the current (working) directory.	N/A
type	Displays the contents of a file.	N/A

PDT special commands: special purpose PDT commands

The following table lists the PDT special purpose PDT commands in the PDT special command group. These commands are in addition to the OAM commands listed in OAM special commands: special purpose PDT commands on page 568.

Table 49: PDT special commands

Command	Description	Element Manager
`reboot [-1]`	Warm reboots the system. Cold reboots the system if the -1 parameter is specified.	N/A
`pins [handle]`	Puts a patch that has been loaded into memory (using the pload command) into service, where [handle] is the number returned by the pload command. If the command is issued without a parameter, you are prompted to enter a [handle]. If issued successfully, the command indicates the global procedures, functions, or areas of memory affected by the patch. You are then prompted and have the choice to proceed or not to proceed.	N/A
`plis [handle]`	Lists detailed patch status information for a loaded patch. If the command is issued without a parameter, you are prompted to enter a [handle].	N/A
`pload ["patch-filename"]`	Loads a patch file from the file system in Flash memory into DRAM memory, where [patch-filename] is the filename or path of the patch file. If a filename alone is provided, the patch must be in the /C:/u/patch directory. Otherwise, the full or relative path can be provided. When a patch is successfully loaded, the command returns a patch handle number. The patch handle number is used as input to other patch commands (pins, poos, pout, and plis). The loaded patch is inactive until it is put into service using the pins command. If the command is issued without a parameter, you are prompted for the patch filename and other information.	N/A

Command	Description	Element Manager
pnew	Creates memory patches for the Media Gateway Card. The command has no parameter(s). The release of the patch is assumed to be the same as that of the current load. The address to be patched is checked to ensure that it is in range. For each address that is changed, the "old" contents are assumed to be the current contents of that memory address. If a path is not provided for the new path filename then it is assumed that the patch is in the /C:/u/patch directory. Once a memory patch is created using the pnew command, it can be loaded and activated like any other patch.	N/A
poos [handle]	Deactivates a patch (takes it out-of-service) by restoring the patched procedure to its original state. If the poos command is issued without a parameter, you are prompted to enter a [handle].	N/A
pout [handle]	Removes a patch from DRAM memory. The patch must be taken out-of-service (using the poos command) before it can be removed from the system. If the pout command is issued without a parameter, you are prompted to enter a handle.	N/A
pstat [handle]	Displays summary status information for one or all loaded patches. For each patch, the following information is displayed: patch handle, filename, reference number, whether the patch is in-service or out-of-service, the reason why the patch is out-of-service (if applicable), and whether the patch is marked for retention or not. Patch retention means that if a reset occurs, then the patch is automatically reloaded into memory and its state (active or inactive) is restored to what it was prior to the system going down. If the [handle] is provided, only the information for the specified patch is displayed. If the command is issued without	N/A

Command	Description	Element Manager
	a parameter, information for all the patches is displayed.	

PDT Security commands: Intrasystem and cryptographic key support

The following table lists the PDY intrasystem and cryptographic key support commands in the PDT Security command group. These commands are in addition to the OAM commands listed in OAM Security commands: Intrasystem and cryptographic key support on page 569

Table 50: PDT Security commands

Command	Description	Element Manager
`sshkeyshow`	Displays the SSH key.	Y
`sshKeyClear`	Clears the SSH key	Y
`sshKeyGenerate`	Generates the SSH key	Y
`joinSecDomain`	Establish mutual trust with the Primary Security Server.	N/A
`leaveSecDomain`	Remove the Primary Security Server mutual trust information from the device.	N/A
`statSecDomain`	Show the Primary Security Server IP address and fingerprint.	N/A

Chapter 36: Media Gateway Controller command line interface commands

Contents

This section contains information on the following topics:

- Introduction on page 582
- Level One (OAM) CLI commands on page 582
  - OAM Command groups on page 582
  - OAM General commands: General purpose on page 583
  - OAM System commands: MGC platform administration and maintenance on page 584
  - OAM VGW commands: Voice Gateway application administration and maintenance on page 585
  - OAM Special commands: special purpose PDT on page 586
  - OAM Security commands: intrasystem and cryptographic key support on page 587
- Level Two (LDB) CLI commands on page 591
  - LDB Command groups on page 591
  - LDB General commands: general purpose on page 592
  - LDB system commands: MGC platform administration and maintenance on page 593
  - LDB Debug commands: PDT debug on page 593
  - LDB disk commands: disk and file commands on page 594
  - LDB special commands: special purpose PDT commands on page 595
  - LDB Security commands: intrasystem and cryptographic key support commands on page 597

Introduction

This chapter identifies and describes the Command Line Interface (CLI) commands available on Gateway Controller cards in the Level One (Operations, Administration, and Maintenance [OAM]) and Level Two (Local Debug [LDB]) security shells. Gateway Controller cards can be Media Gateway Controller (MGC) card, Common Processor Media Gateway (CP MG) card, and Media Gateway Extended Peripheral Equipment Controller (MG XPEC) card.

The information in this chapter is presented in tables organized by Command Groups. Command Groups group together commands of similar functionality or purpose within a security shell. Each table relates to a particular Command Group and contains the associated commands, a description of each command, and an indication of whether the command is available through the Element Manager interface.

Level One (OAM) CLI commands

This section lists the Command Groups and commands available in the Level One (Operations, Administration, and Maintenance [OAM]) security shell. The OAM security shell can only be accessed if your password is configured for OAM access. To access the OAM security shell, you must force the MGC logon prompt to appear by holding down the CTRL key and typing **`oam`**. The prompt for each command in the OAM security shell is **`'oam>'`**.

The following section identifies the Command Groups in the OAM security shell. All subsequent sections are specific to a given OAM Command Group and describe the commands in the Command Group.

OAM Command groups

The following table lists the Command Groups available in the OAM security shell. To display a list of these Command Groups, type **`help`** at the OAM security shell prompt.

Some of the Command Groups that are displayed in the OAM security shell contain commands that are only available in the LDB security shell. These Command Groups are italicized in the following table.

Table 51: OAM CLI command groups

Command group	Description	Commands
General	General purpose commands.	Table 52: OAM General commands on page 583
System	Gateway Controller platform administration and maintenance commands.	Table 53: OAM system commands on page 584
VGW	Voice Gateway application administration and maintenance commands.	Table 54: OAM VGW commands on page 585
Debug	PDT Debug commands	Not available in OAM security shell.
Disk	Disk and file commands	Not available in OAM security shell.
Special	Special purpose PDT commands.	Table 55: OAM Special commands on page 586
Security	Intrasystem and cryptographic key support commands.	Table 56: OAM Security commands on page 587

OAM Commands

The following tables list the commands available within each Command Group in the OAM security shell. To display a list of commands in a specific OAM Command Group, type **`help <command group name>`** at the OAM security shell prompt.

OAM General commands: General purpose

The following table lists the OAM general purpose commands in the OAM General Command Group.

Table 52: OAM General commands

Command	Description	Element Manager
`exit`	Terminate current shell.	N/A
`help`	Show a list of available Command Groups.	N/A

Command	Description	Element Manager
version	Display VxWorks™ version, date of build, and other information.	Y

OAM System commands: MGC platform administration and maintenance

The following table lists the OAM Gateway Controller platform administration and maintenance commands in the OAM System Command Group.

Table 53: OAM system commands

Command	Description	Element Manager
macshow	Displays all of the MAC addresses associated with the Ethernet ports (both internal and external) on the embedded Ethernet switch.	Y
diskshow	Displays the total, used and available disk space available on the internal compact flash card.	Y
memshow	Displays the total, used and available RAM memory.	Y
ethportshow	Displays the Ethernet port settings for the external and internal interfaces, including autonegotiation settings, duplex, port speed and port mirroring status.	N/A
ethspeedshow	Displays the port speed and duplex setting for the ports of the embedded Ethernet switch.	Y
dbhwshow	Displays the model and revision numbers for installed Daughterboards.	Y
diskformat	Formats the internal compact flash on the Gateway Controller.	N/A
rmonstatshow [port]	Displays the RMON statistics collected by the embedded Ethernet switch for a given port.	Y
rmonstatshowall	Displays the RMON statistics collected by the embedded Ethernet switch for all ports.	Y
rmonstatreset [port]	Resets all RMON statistics counters on the embedded Ethernet switch for a given port.	Y
rmonstatresetall	Resets all RMON statistics counters for all ports on the embedded Ethernet switch.	Y
mgcsetup	Starts the MGC setup menu, allowing modifications to the local Gateway Controller	N/A

Command	Description	Element Manager
	configuration information, including local IP addresses, hostname and Call Server IP address.	
`swversionshow`	Displays all of the versions of software/loadware currently in service on the Gateway Controller.	Y
`displayshow`	Displays all messages currently being displayed on the 4 character LED of this Gateway Controller, except the superloop and shelf.	Y
`mspversionshow`	Displays the MSP device type, ARM code, voice DSP revision, and T.38 version.	Y

OAM VGW commands: Voice Gateway application administration and maintenance

The following table lists the OAM Voice Gateway application administration and maintenance commands in the OAM VGW Command Group.

Table 54: OAM VGW commands

Command	Description	Element Manager
`dspnumshow`	Displays the number of DSP channels for each DSP Daughterboard.	Y
`dspchanstateshow`	Displays the state of all the channels on the DSP Daughterboards. This is analogous to the itgChanStateShow command for VGMC cards.	Y
`dsphwcheck`	Perform a basic DSP hardware diagnostic check.	Y
`dsplooptest [channel1 channel2]`	Perform DSP loopback test for all inactive channels, or for the channels entered.	Y
`vgwshow`	Displays information about busy gateway channels. Entering this command with the IP address of an etherset at the CLI of any node's ITGL card displays the identification of the card that has a gateway channel in use by the etherset. This is useful when you need to identify which card to collect gateway statistics (like packet loss, etc.) from, for instance.	Y

Command	Description	Element Manager
`vgwshowall`	Displays status information about all gateway channels on a VGMC card / DSP Daughterboard.	Y
`vgwcardshow [card number]`	Displays information about voice gateway channels on a VGMC card / DSP Daughterboard.	Y
`ommshow`	Displays the contents of the OMREPORT.nnn file, that contains the operational measurements for the VGW channels.	Y

OAM Special commands: special purpose PDT

The following table lists the OAM special purpose PDT commands in the OAM Special Command Group.

Table 55: OAM Special commands

Command	Description	Element Manager
`testalarm`	Tests SNMP traps.	Y
`rdhelp`	Lists all report display commands.	N/A
`rdopen [filename]`	Opens a report log file. Where [filename] is the name of the report file to be opened.	Y
`rdgo [N]`	Goes to a specific record. Where [N] is the absolute record number.	Y
`rd [S] [R]`	Displays a specified number of records starting at a specified point. Where: • [S] is the number of steps to traverse to the starting point. • [R] is the number of records to display. Both [S] and [R] can be negative.	Y
`rds [S] [R]`	Displays a specified number of records, with a symbolic dump, starting at a specified point. Where: • [S] is the number of steps to traverse to the starting point. • [R] is the number of records to display.	Y

Command	Description	Element Manager
	Both [S] and [R] can be negative.	
`rdshow`	Displays general information about the current log file and the current rd settings.	Y
`rdall`	Displays all records.	N/A
`rdtail [N]`	Displays the specified number of newest records. Where [N] is the number of records to display.	Y
`rdhead [N]`	Displays the specified number of oldest records. Where [N] is the number of records to display.	Y
`rdnext`	Opens the next log file.	Y
`rdprev`	Opens the previous log file.	Y
`rdsconvert [filename]`	Converts a log file to text. Where [filename] is the name of the log file to be converted.	Y

OAM Security commands: intrasystem and cryptographic key support

The following table lists the OAM intrasystem and cryptographic key support commands in the OAM Security Command Group.

Table 56: OAM Security commands

Command	Description	Element Manager
`disInsecureShells`	Disables all insecure shells in the system	Y
`disSecureShells`	Disable all secure shells in the system	Y
`enlInsecureShells`	Enable all insecure shells in the system	Y
`enlSecureShells`	Enables all secure shells in the system	Y
`isecChgPSK`	Changes ISEC PSK locally.	Y
	Changing the local ISEC configuration can cause a temporary ELAN outage which would last until all connected elements share the same configuration. This would affect established calls and IP based terminal sessions.	

Command	Description	Element Manager
	Note: If this command is running on one of the CPU's in a redundant CS, the change is not synchronized with the other core.	
`isecChgLevel [OPTI/FUNC/FULL]`	Changes ISEC security level locally. Changing the local ISEC configuration can cause a temporary ELAN outage which would last until all connected elements share the same configuration. This would affect established calls and IP based terminal sessions. **Note:** If this command is running on one of the CPU's in a redundant CS, the change is not synchronized with the other core. Where: • OPTI = Optimized Security Only the pbxLink and XMSG ports are encrypted using IPsec for a given IP address, and unencrypted traffic is permitted on all other ports. This applies to the Embedded Local Area Network (ELAN) ports only. • FUNC = Functional Security All links between all known addresses are encrypted using IPsec (except SSH, SSL, AML, NTP). Unencrypted links from any other IP address are permitted. • FULL = Full Security (Standard Mode) All links between all known addresses are encrypted using IPsec (except SSH, SSL, AML, NTP). Links from any other IP address are encrypted using ISSS. **Note:** Known addresses are those IP addresses that are part of the node configured in Element Manager, or that are present in the list of trusted hosts.	Y
`isecconfirm`	Used to confirm PSK between Active Call Server and other elements. The salt value, hashed PSK, system security status and system level appear.	Y

Command	Description	Element Manager
`isecNewTarget [IP Address]`	Adds a new target to the ISEC target list. Changing the local ISEC configuration can cause a temporary ELAN outage which would last until all connected elements share the same configuration. This would affect established calls and IP based terminal sessions. Where: [IP Address] identifies a specific target's IP address. **Note:** If this command is running on one of the CPU's in a redundant CS the change is not synchronized with the other core.	Y
`isecOutTarget [IP Address]`	Deletes a target from the ISEC target list. Changing the local ISEC configuration can cause a temporary ELAN outage which would last until all connected elements share the same configuration. This would affect established calls and IP based terminal sessions. Where: [IP Address] identifies a specific target's IP address. **Note:** If this command is running on one of the CPU's in a redundant CS the change is not synchronized with the other core.	Y
`isecEnlTarget [IP Address]`	Enables the ISEC target. Where: [IP Address] identifies a specific target's IP address. **Important:** This command returns an error in either of the following cases: • If no system secret exists, the system returns an error indicating that you must run the CHG ISEC PSK command to configure a system secret. • If no security option exists, the system returns an error indicating that you must run	Y

Command	Description	Element Manager
	the isecChgPSK command to configure a security option.	
`isecDisTarget [IP Address]`	Disables the ISEC target. Changing the local ISEC configuration can cause a temporary ELAN outage which would last until all connected elements share the same configuration. This would affect established calls and IP based terminal sessions. Where: [IP Address] identifies a specific target's IP address. **Note:** If this command is running on one of the CPU's in a redundant CS the change is not synchronized with the other core.	Y
`isecProfileShow`	Displays all ISEC profiles.	Y
`isecDecom`	Removes all ISEC related files, memory allocations, and tasks.	Y
`isecIkeShowPAll`	Displays all protection suites (inbound and outbound IPsec Security Association pairs).	Y
`isecIpsecShowIf`	Displays all of the network interfaces on which IPsec is enabled. For each session, the following information appears: • Interface name • IP address • DF bit status	Y
`sshKeyActivate`	Activate the SSH key	Y
`sshKeyShow`	Displays the fingerprint of the public key of the MGC. Displays both active and pending keys.	Y
`sshKeyClear`	Clears the SSH key	Y
`sshKeyGenerate`	Generate the SSH key	Y
`statInsecureShells`	Displays whether insecure shell access is enabled or disabled.	Y
`statSecureShells`	Displays whether secure shell access is enabled or disabled.	Y

Command	Description	Element Manager
statSecDomain	Show the Primary Security Server IP address and fingerprint.	N/A

Level Two (LDB) CLI commands

The Level Two (Local Debug [LDB]) security shell can only be accessed if your password is configured for LDB security shell access. To access the LDB security shell, you must force the MGC logon prompt to appear by holding down the CTRL key and typing **ldb**. The prompt for each command in the LDB security shell is **'ldb>'**.

This section contains tables corresponding to Command Groups that are available in the LDB security shell. LDB security shell capabilities are inclusive of all OAM security shell capabilities. All Level One (OAM) Gateway Controller CLI Command Groups and associated commands are available in the Level Two (LDB) security shell by definition.

This section contains tables representing two categories of Command Groups:

- those containing commands that are available in both the OAM and LDB security shells

  Commands that are available in the OAM security shell are not repeated in these Command Group tables. See the equivalentLevel One (OAM) CLI commands on page 582 Command Group table for descriptions of these commands.

- those containing commands that are only available in the LDB security shell

LDB Command groups

The following table lists the LDB Command Groups. Command groups that contain commands that are only available in the LDB security shell are in italics. To display a list of commands in a specific Command Group, type **help <command group name>** at the prompt.

Table 57: LDB CLI command groups

Command group	Description	LDB Commands
General	General purpose commands.	Table 58: LDB General commands on page 592
System	Gateway Controller platform administration and maintenance commands.	Table 59: LDB system commands on page 593

Command group	Description	LDB Commands
Debug	PDT debug commands.	Table 60: LDB Debug commands on page 594
Disk	Disk and file commands.	Table 61: LDB disk commands on page 594
Special	Special purpose PDT commands.	Table 62: LDB special commands on page 595
Security	Intrasystem and cryptographic key support commands.	LDB Security commands: intrasystem and cryptographic key support commands on page 597

LDB Commands

The following tables list the commands in each Command Group in the LDB security shell. To display a list of commands in a specific LDB Command Group, type **help <command group name>** at the prompt.

LDB General commands: general purpose

The following table lists the PDT general purpose commands in the LDB General Command Group. These commands are in addition to the OAM commands listed in OAM General commands: General purpose on page 583.

Table 58: LDB General commands

Command	Description	Element Manager
devs	Displays the list of devices.	N/A
echo	Echo the inputs..	N/A
h	Displays the 20 most recent commands entered in the shell.	N/A
hosts	Displays a list of hosts.	Y

Command	Description	Element Manager
`i`	Displays a summary of task control block information.	N/A
`mem`	Displays memory usage and a list of free blocks.	N/A
`rdaccess`	Displays shell access attempts.	N/A
`rx`	Receive a file over a serial connection using XMODEM.	N/A
`ti [name | taskid]`	Displays task information for a specified task. Where: • [name] is the name of the task. • [taskID] is the ID of the task. [name] and [taskID] are mutually exclusive.	N/A

LDB system commands: MGC platform administration and maintenance

The following table lists the LDB MGC platform administration and maintenance commands in the LDB system Command Group. These commands are in addition to the OAM commands listed in OAM System commands: MGC platform administration and maintenance on page 584.

Table 59: LDB system commands

Command	Description	Element Manager
`ethportmirror [port1] [port2]`	Allows mirroring of one of the embedded Ethernet switch ports. To disable mirroring of a port, use ‘none’ for port2.	N/A
`ethportdisable [port]`	Disables a port so it can be used for mirroring.	N/A
`ethportreset`	Clears all port mirroring and reenables standard embedded Etherenet switch functionality.	N/A
`ethportcabletest`	Test the cable connected to the port	N/A

LDB Debug commands: PDT debug

The following table lists the LDB PDT debug commands in the LDB Debug Command Group.

Table 60: LDB Debug commands

Command	Description	Element Manager
`td`	Deletes a task.	N/A

LDB disk commands: disk and file commands

The following table lists the LDB disk and file commands in the LDB disk Command Group.

Table 61: LDB disk commands

Command	Description	Element Manager
`cd [path]`	Changes the default directory. Where: [path] = the path and name of the new directory. The [path] of the new directory can be specified as a relative path.	N/A
`chkdsk`	Checks file system consistency. chkdsk "/C:" Checks the internal file system for errors. chkdsk "/C:", 1 Repairs the file system errors and saves the damaged cluster in files. chkdsk "/C:", 2 Repairs file system errors and returns damaged clusters to the free pool.	Y
`cp`	Copies multiple files to another directory.	N/A
`copy [input] [output]`	Copies from one file to another file until an end-of-file (CTRL+d) is reached. Where: • [input] = the name of the file to be copied from. If NULL, stdin is used. • [output] is the name of the new or destination file to be copied to. If NULL, stdout is used.	N/A
`label`	Creates, displays, or changes a device label.	N/A
`ll [path]`	Displays a long list of the contents of a directory.	N/A

Command	Description	Element Manager
	Where: [path] = the path name of the directory. If path is not specified, the contents of the current directory are displayed.	
`ls [path]`	Displays the contents of a directory. Where: [path] = the path name of the directory. If [path] is not specified, the contents of the current directory are displayed.	N/A
`pwd`	Displays the current (working) directory.	N/A
`type`	Displays the contents of a file.	N/A

LDB special commands: special purpose PDT commands

The following table lists the LDB special purpose PDT commands in the LDB special Command Group. These commands are in addition to the OAM commands listed in OAM Special commands: special purpose PDT on page 586.

Table 62: LDB special commands

Command	Description	Element Manager
`reboot [-1]`	Warm reboots the system. Cold reboots the system if the -1 parameter is specified.	N/A
`pins [handle]`	Puts a patch that has been loaded into memory (using the pload command) into service, where [handle] is the number returned by the pload command. If the command is issued without a parameter, you are prompted to enter a [handle]. If issued successfully, the command indicates the global procedures, functions, or areas of memory affected by the patch. You are then prompted and have the choice to proceed or not to proceed.	N/A
`plis [handle]`	Lists detailed patch status information for a loaded patch.	N/A

Command	Description	Element Manager
	If the command is issued without a parameter, you are prompted to enter a [handle].	
`pload "[patch-filename]"`	Loads a patch file from the file system in Flash memory into DRAM memory, where [patch-filename] is the filename or path of the patch file. If a filename alone is provided, the patch must be in the /C:/u/patch directory. Otherwise, the full or relative path can be provided. When a patch is successfully loaded, the command returns a patch handle number. The patch handle number is used as input to other patch commands (pins, poos, pout, and plis). The loaded patch is inactive until it is put into service using the pins command. If the command is issued without a parameter, you are prompted for the patch filename and other information.	N/A
`pnew`	Creates memory patches for the Gateway Controller card. The command has no parameter(s). The release of the patch is assumed to be the same as that of the current load. The address to be patched is checked to ensure that it is in range. For each address that is changed, the "old" contents are assumed to be the current contents of that memory address. If a path is not provided for the new path filename then it is assumed that the patch is in the /C:/u/patch directory. Once a memory patch is created using the pnew command, it can be loaded and activated like any other patch.	N/A
`poos [handle]`	Deactivates a patch (takes it out-of-service) by restoring the patched procedure to its original state. If the poos command is issued without a parameter, you are prompted to enter a [handle].	N/A
`pout [handle]`	Removes a patch from DRAM memory. The patch must be taken out-of-service (using the poos command) before it can be removed from the system.	N/A

Command	Description	Element Manager
	If the pout command is issued without a parameter, you are prompted to enter a handle.	
`pstat [handle]`	Displays summary status information for one or all loaded patches. For each patch, the following information is displayed: patch handle, filename, reference number, whether the patch is in-service or out-of-service, the reason why the patch is out-of-service (if applicable), and whether the patch is marked for retention or not. Patch retention means that if a reset occurs, then the patch is automatically reloaded into memory and its state (active or inactive) is restored to what it was prior to the system going down. If the [handle] is provided, only the information for the specified patch is displayed. If the command is issued without a parameter, information for all the patches is displayed.	N/A

LDB Security commands: intrasystem and cryptographic key support commands

The following table lists the LDB Security commands in the LDB Security Command Group. These commands are in addition to the OAM commands listed in OAM Security commands: intrasystem and cryptographic key support on page 587.

Table 63: LDB Security commands

Command	Description	Element Manager
`joinSecDomain`	Establish mutual trust with the Primary Security Server.	N/A
`leaveSecDomain`	Remove the Primary Security Server mutual trust information from the device.	N/A

Chapter 37: Signaling Server Command Line Interface commands

Contents

This section contains information on the following topics:

- Introduction on page 600
- Level One (OAM) CLI commands on page 601
  - OAM Command groups on page 601
  - OAM DLOG commands: Firmware download log file on page 604
  - OAM GK commands: Gatekeeper on page 605
  - OAM Network commands: remote access on page 611
  - OAM Patcher commands: patching on page 611
  - OAM SSH commands: SSH commands on page 612
  - OAM UFTP commands: UFTP IP Phone firmware download on page 612
  - OAM cds commands: Converged Desktop Service Module on page 614
  - OAM elm commands: ELM module on page 615
  - OAM emhelp commands: Element Manager help file related commands on page 615
  - OAM iset commands: iset module on page 615
  - OAM mam commands: MAM module on page 617
  - OAM ncs commands: Network Connection Service module on page 621
  - OAM npm commands: Network Protocol Module on page 623
  - OAM nrsDB commands: Network Routing Service on page 626
  - Table 79: OAM nrsomm commands on page 627
  - OAM pbxlink commands: PBX link on page 627
  - OAM securityShell commands: Security shell on page 628
  - OAM sipcti commands: SIP CTI module commands on page 628

- OAM sipctiomm commands: SIP CTI OMM commands on page 630
- OAM sipnpm commands: SIP Network Protocol Module on page 631
- OAM system commands: system administration commands on page 635
- OAM tps commands: TPS module on page 637
- OAM trace commands: General trace tools on page 638
- OAM uipc commands: Universal ISDN Protocol module on page 639
- OAM ums commands: UMS module on page 640
- OAM usi commands: RUDP timeout and retry commands on page 641
- OAM vte commands: Virtual Terminal Emulator on page 642
- OAM vtrk commands: Virtual Trunk module on page 642
- OAM cds commands: Converged Desktop Service module commands on page 643

• Level Two (PDT) CLI commands on page 645

- PDT Command groups on page 645
- Accounts commands: user account administration commands on page 647
- disk commands: file system maintenance and diagnostics on page 652
- rdtools commands: rd tools on page 655
- PDT nrsDB commands: Network Routing Service on page 652
- PDT sipnpm commands: SIP Network Protocol Module on page 656
- PDT system commands: System administration on page 658
- PDT ums commands : UMS module commands on page 660
- PDT iset commands: iset module commands on page 661

• CLI commands in Linux on page 663

Introduction

This chapter lists and describes the Command Line Interface (CLI) commands available on the Signaling Server platform in the Level One (OAM) and Level Two (PDT) security shells.

The OAM security shell can only be accessed if your password is configured for Level One (OAM) access. The CLI command prompt in the OAM security shell is **`oam>`**. Similarly, the PDT security shell can only be accessed if your password is configured for Level Two (PDT) access. The CLI command prompt in the PDT security shell is **`pdt>`**.

If you have Level Two (PDT) security shell access, you automatically have Level One (OAM) security shell access. To access the PDT security shell from the OAM security shell, hold down the CTRL button and type **pdt** at the command prompt in the OAM security shell.

The information in this chapter is presented in the form of CLI Command Groups. CLI Command Groups are used to group together commands of similar functionality or purpose. Each CLI Command Group is represented by a table that lists all associated CLI commands with a detailed command description. Each table contains a column indicating whether or not a listed CLI command can be executed through the General Command interface of the Element Manager application on the Signaling Server.

Level One (OAM) CLI commands

This section describes the CLI Command Groups and commands available in the Level One (Operations, Administration, and Maintenance [OAM]) security shell. To display a list of the Command Groups available in the OAM security shell, type **help** at the OAM security shell command prompt (**oam>**). To display a list of commands in an OAM security shell Command Group, type **help <command group name>** at the OAM security shell command prompt.

OAM Command groups

The following table lists the Command Groups available in the OAM security shell. To display a list of the Command Groups available in the OAM security shell, type **help** at the OAM security shell command prompt.

Table 64: OAM CLI command groups

Command group	Description	Commands
DLOG	Firmware download log file commands	Table 65: OAM DLOG commands on page 604
GK	Gatekeeper module commands	Table 66: OAM GK commands on page 605
Network	Remote access commands	Table 67: OAM Network commands on page 611
Patcher	Patch commands	Table 68: OAM Patcher commands on page 612

Command group	Description	Commands
SSH	SSH commands	Table 69: OAM SSH commands on page 612
UFTP	UFTP IP Phone firmware download commands.	Table 70: OAM UFTP commands on page 613
cds	Converged Desktop Service module commands	Table 71: OAM cds commands on page 614
elm	ELM module commands	Table 72: OAM elm commands on page 615
emhelp	EM Help File related commands	Table 73: OAM emhelp commands on page 615
iset	iset module commands	Table 74: OAM iset commands on page 615
mam	MAM module commands	Table 75: OAM mam commands on page 618
ncs	Network Connection Service module commands	Table 76: OAM ncs commands on page 621
npm	Network Protocol Module commands	Table 77: OAM npm commands on page 623
nrsDB	Network Routing Service commands	Table 78: OAM nrsDB commands on page 626
nrsomm	Network Routing Service operational measurement commands	Table 79: OAM nrsomm commands on page 627
pbxlink	PBX link commands	Table 80: OAM pbxlink commands on page 628
securityShell	Security shell commands	Table 81: OAM securityShell commands on page 628

Command group	Description	Commands
sipcti	SIP CTI module commands	Table 82: OAM sipcti commands on page 629
sipctiomm	SIP CTI OMM display commands	Table 83: OAM sipctiomm commands on page 631
sipnpm	SIP Network Protocol Module commands	Table 84: OAM sipnpm commands on page 631
system	System administration commands	Table 85: OAM system commands on page 635
tps	TPS module commands	Table 86: OAM tps commands on page 637
trace	General trace tools	Table 87: OAM trace commands on page 638
uipc	Universal ISDN module commands	Table 88: OAM uipc commands on page 639
ums	UMS module commands	Table 89: OAM ums commands on page 640
usi	RUDP timeout and retry commands	Table 90: OAM usi commands on page 641
vte	Virtual Terminal Emulator commands	Table 91: OAM vte commands on page 642
vtrk	Virtual Trunk module commands	Table 92: OAM vtrk commands on page 642
cds	Converged Desktop Services commands	Table 93: OAM cds commands on page 643

OAM Commands

The following tables list the commands in each Command Group at the OAM access level. To display a list of commands in a specific OAM Command Group, type **help <command group name>** at the prompt.

OAM DLOG commands: Firmware download log file

The following table lists the OAM firmware download log file commands in the OAM DLOG command group.

Table 65: OAM DLOG commands

Command	Description	Element Manager
activeDlogShow [numOfLine]	Displays the active DLOG file information for UFTP IP Phone firmware downloads. Where: [numOfLine] = the number of lines of the active DLOG file to display. When [numOfLine] parameter is not used, the output displays the contents of the entire active DLOG file.	N/A
inactiveDlogShow [numOfLine]	Displays the inactive DLOG file information for UFTP IP Phone firmware downloads. Where: [numOfLine] = the number of lines of the inactive DLOG file to display. When [numOfLine] parameter is not used, the output displays the contents of the entire inactive DLOG file.	N/A
dnldFailShow [numOfLine]	Displays the "download failed" entries logged in the active and inactive DLOG files. Where: [numOfLine] = the number of lines of "download failed" entries in the active and inactive DLOG files to display When [numOfLine] parameter is not used, the output displays all "download failed" entries in the active and inactive DLOG files.	N/A

OAM GK commands: Gatekeeper

The following table lists the OAM Gatekeeper commands in the OAM GK command group.

Table 66: OAM GK commands

Command	Description	Element Manager
`gkDiscoveryTrace [endpoint type]`	Initiates discovery tracing for a specified GK endpoint type. Outputs the GRQ, GCF, and GRJ messages for the specified GK endpoint type. Where [endpoint type] is: • ID ["Alias Name"] Initiates discovery tracing for a specified GK endpoint, where "Alias Name" is the H.323 GK ID of the endpoint. • IP ["IP address"] Initiates discovery tracing for a specified GK endpoint, where "IP address" is the IP address of the endpoint. • ALL Initiates discovery tracing on all GK endpoints.	N/A
`gkRegTrace [endpoint type]`	Initiates registration tracing for a specified GK endpoint type. Outputs the RRQ, RCF, RRJ, URQ, UCF, and URJ messages for the specified GK endpoint type. Where [endpoint type] is: • ID ["Alias Name"] Initiates registration tracing for a specified GK endpoint, where "Alias Name" is the H.323 GK ID of the endpoint. • IP ["IP address"] Initiates registration tracing for a specified GK endpoint, where "IP address" is the IP address of the endpoint. • ALL Initiates registration tracing on all GK endpoints.	N/A
`gkCallTrace [endpoint type]`	Initiates call tracing for a specified GK endpoint type.	N/A

Command	Description	Element Manager
	Outputs the ARQ, ACF, ARJ, LRQ, LCF, LRJ, BRQ, BCF, BRJ, DRQ, DCF, and DRJ messages for the specified GK endpoint type. Where [endpoint type] is: • ID ["Alias Name"] Initiates call tracing for a specified GK endpoint, where "Alias Name" is the H.323 GK ID of the endpoint. • IP ["IP address"] Initiates call tracing for a specified GK endpoint, where "IP address" is the IP address of the endpoint. • NUM [calling/called number] Initiates call tracing for a number, regardless of NPI and TON. The [calling/called number] value can be a number from 1 to 32 digits. It can be a partial number. • NUM [calling/called number] [NPI] [TON] Initiates call tracing for a number with a particular TON and NPI. [NPI] specifies the Numbering Plan Identifier to use as a filter for tracing. The values are: - 0 - ALL - 1 - Unknown - 2 - ISDN/telephony numbering plan (E.164) - 3 - Private numbering - 4 - E.163 - 5 - Telex numbering plan (F.69) - 6 - Data numbering plan - 7 - National standard numbering plan [TON] specifies the Type Of Number to use as a filter for tracing. The values are: - 0 - ALL - 1 - Unknown Number - 2 - International Number - 3 - National Number - 4 - Network Specific Number - 5 - Subscriber Number	

Command	Description	Element Manager
	- 6 - Level 1 Regional - 7 - Level 0 Regional (Abbreviated number) • ALL Initiates tracing on all GK endpoints. **Note:** A maximum of ten number traces are allowed.	
`gkProtocolTrace [endpoint type] [protocol]`	Initiates protocol tracing for a specified GK endpoint type. Where [endpoint type] is: • ID ["Alias Name"] Initiates protocol tracing for a specified GK endpoint, where "Alias Name" is the H.323 GK ID of the endpoint. • IP ["IP address"] Initiates protocol tracing for a specified GK endpoint, where "IP address" is the IP address of the endpoint. • NUM [calling/called number] Initiates protocol tracing for a number, regardless of NPI and TON. The [calling/called number] value can be a number from 1 to 32 digits. It can be a partial number. • NUM [calling/called number] [NPI] [TON] Initiates protocol tracing for a number with a particular TON and NPI. [NPI] specifies the Numbering Plan Identifier to use as a filter for tracing. The values are: - 0 - ALL - 1 - Unknown - 2 - ISDN/telephony numbering plan (E.164) - 3 - Private numbering - 4 - E.163 - 5 - Telex numbering plan (F.69) - 6 - Data numbering plan - 7 - National standard numbering plan	N/A

Command	Description	Element Manager
	[TON] specifies the Type Of Number to use as a filter for tracing. The values are: - 0 - ALL - 1 - Unknown Number - 2 - International Number - 3 - National Number - 4 - Network Specific Number - 5 - Subscriber Number - 6 - Level 1 Regional - 7 - Level 0 Regional (Abbreviated number) • ALL Initiates protocol tracing on all GK endpoints. Where [protocol] specifies the protocol to trace. • Individual protocols for IP, ID and ALL protocol tracing: ALL, ARQ, ACF, ARJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ, GRQ, GCF, GRJ, LRQ, LCF, LRJ, NSM, RRQ, RCF, RRJ, RIP, URQ, UCF, and URJ • Protocol categories for IP, ID, and ALL protocol tracing - AXX – ARQ, ACF, ARJ - BXX – BRQ, BCF, BRJ - DXX – DRQ, DCF, DRJ - GXX – GRQ, GCF, GRJ - LXX – LRQ, LCF, LRJ - RXX – RRQ, RCF, RRJ - UXX – URQ, UCF, URJ • Individual protocols for NUM protocol tracing: ALL, ARQ, ACF, ARJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ,LRQ, LCF, LRJ • Protocol categories for NUM protocol tracing: - AXX – ARQ, ACF, ARJ - BXX – BRQ, BCF, BRJ - DXX – DRQ, DCF, DRJ	

Command	Description	Element Manager
	- LXX – LRQ, LCF, LRJ • Protocols that can't be traced by any endpoint: IACK, INAC, IRQ, IRR, RAI, RAC, SCI, SCR, XRS **Note:** A maximum of ten number traces are allowed.	
`gkTraceOff [endpoint type]`	Discontinues all tracing for a specified GK endpoint type. Where [endpoint type] is: • ID ["Alias Name"] Discontinues tracing for a specified GK endpoint, where "Alias Name" is the H.323 GK ID of the endpoint. • IP ["IP address"] Discontinues tracing for a specified GK endpoint, where "IP address" is the IP address of the endpoint. • NUM [calling/called number] Discontinues tracing for a number, regardless of NPI and TON. The [calling/called number] value can be a number from 1 to 32 digits. It can be a partial number. • NUM [calling/called number] [NPI] [TON] Discontinuesl tracing for a number with a particular TON and NPI. [NPI] specifies the Numbering Plan Identifier to use as a filter for tracing. The values are: - 0 - ALL - 1 - Unknown - 2 - ISDN/telephony numbering plan (E.164) - 3 - Private numbering - 4 - E.163 - 5 - Telex numbering plan (F.69) - 6 - Data numbering plan - 7 - National standard numbering plan	N/A

Command	Description	Element Manager
	[TON] specifies the Type Of Number to use as a filter for tracing. The values are: - 0 - ALL - 1 - Unknown Number - 2 - International Number - 3 - National Number - 4 - Network Specific Number - 5 - Subscriber Number - 6 - Level 1 Regional - 7 - Level 0 Regional (Abbreviated number) • ALL Discontinues tracing on all GK endpoints.	
`gkTraceOutput [Output_Destination] ["File Pathname"]`	Specifies the output destination for all Gatekeeper traces. Where: • [Output_Destination] specifies where all the trace messages for the GK traces are to be directed. Values are: - 1 = TTY - 2 = RPTLOG (syslog) - 3 = User-specified FILE in the /u/trace directory. File name must be in quotes and conform to the 8.3 format. - 4 = TTY and user-specified FILE. • ["File Pathname"] specifies the output file name when option 3 or 4 is specified.	N/A
`gkTraceSettings`	Displays the GK trace output destination and the GK endpoint types being traced.	N/A
`gkTraceTblClear`	Clears the calling/called number table associated with the NUM trace filter(s). A maximum of 200 tables entries are allowed. If there are more than 200 table entries, the system displays the following error message: `gkTrace callIdentifier table is full`	N/A

Command	Description	Element Manager
	Clearing the table is a temporary solution. Better options may include: • refining the NUM trace filter to be more exact • reducing the number of NUM trace filters • running the trace during lower traffic periods	
`gkTraceTblShow`	Displays the calling/called number table associated with the NUM trace filter(s). Some entries may be shown twice, since intrazone calls generate two ARQ messages to the primary Gatekeeper. Interzone calls generate only one ARQ message.	N/A

OAM Network commands: remote access

The following table lists the OAM remote access commands in the OAM Network command group.

Table 67: OAM Network commands

Command	Description	Element Manager
`telnet [server] [username]`	Telnets to a server. The address can be either in IP address format or host name. Where: • server = IP address • username = host name	N/A
`rlogin [server] [username]`	Remotely logs in to a server. The address can be either an IP address or host name. Where: • server = IP address • username = host name	N/A
`cslogin`	Logs in to the Call Server overlays.	N/A

OAM Patcher commands: patching

The following table lists the OAM patching commands in the OAM Patcher command group.

Table 68: OAM Patcher commands

Command	Description	Element Manager (see Note)
`mdp`	DEPLIST manipulation command	N/A

Note:
The Patcher command is not available in Element Manager from the Node Maintenance web page. It is available from **IP Telephony > Software > Patching**

OAM SSH commands: SSH commands

The following table lists the OAM SSH commands in the OAM SSH command group.

Table 69: OAM SSH commands

Command	Description	Element Manager
`sshKeyClear`	Clears all of the public keys (active and pending) stored on the Signaling Server. **Important:** You must disable secure shells before you can clear SSH keys.	Y
`sshKeyGenerate`	Generates the SSH key on the Signaling Server. **Important:** The generated key is stored in a pending state until it is activated.	Y
`sshKeyShow`	Displays the fingerprint of the public key of the Signaling Server. Displays both active and pending keys.	Y

OAM UFTP commands: UFTP IP Phone firmware download

The following table lists the OAM UFTP IP Phone firmware download commands in the OAM UFTP command group.

These OAM UFTP commands are used with a Signaling Server in maintenance mode. When the Signaling Server is in maintenance mode, the maximum number of simultaneous firmware downloads is increased, thereby allowing the UNIStim Firmware Transfer Protocol (UFTP) server to use most of its processing resources.

Table 70: OAM UFTP commands

Command	Description	Element Manager
`uftpShow`	Displays IP Phone firmware download information. • configuration information about UFTP • count of successful downloads since a Signaling Server reboot • count of downloads that failed or prematurely ended since a Signaling Server reboot • number of active downloads, and a list of each, including: - type of IP Phone - IP addresses of the IP Phones that downloaded firmware - number of bytes downloaded	N/A
`uftpRunTimeDataReset`	Resets the run time data field in the UFTP data block.	N/A
`uftpTurboMode ["HH:MM/start/stop/on/off"] [MM] ["show"]`	Configures maintenance mode. Where: • "HH:MM" – time to enter Maintenance Mode in 24-hour format • "start" – enter Maintenance Mode immediately • "stop" – stop Maintenance Mode • "on" – allow Signaling Server to enter Maintenance Mode • "off" – do not allow Signaling Server to enter Maintenance Mode • MM – optional parameter that defines the length of time in minutes that Maintenance Mode is to be maintained • "show" – displays the same output as uftpTurboModeShow If no parameter is entered, Upgrade Manager defaults to uftpturboMode "start".	Y
`uftpTurboModeShow`	Displays the current status of maintenance mode.	Y
`uftpSpeedLimitShow`	Display UFTP bandwidth parameters.	N/A

Command	Description	Element Manager
`uftpSpeedLimitSet`	Configure UFTP bandwidth parameters.	N/A
`uftpTurboModeTimeoutSet [MM]`	Configures the idle timeout timer for maintenance mode. Where: [MM] – optional parameter that defines the number of minutes the Upgrade Manager waits after the last firmware download job is started before returning the Signaling Server to normal mode If this parameter is configured as 0 (zero), the Upgrade Manager never exits Maintenance Mode unless the umsUpgradeModeSet command is issued with the "stop" parameter. If no parameter is entered, then the current timeout setting is displayed.	Y
`uftpAutoUpgradeTimeoutSet [MM]`	Configures the length of time the IP Phone waits for a user response after "Upgrade F/W now?" message is displayed before automatically beginning the firmware upgrade. Where: [MM] – user response timeout in minutes. A value of 0 (zero) means "Print current settings". If no parameter is entered, the current value is printed.	Y

OAM cds commands: Converged Desktop Service Module

The following table lists the OAM Converged Desktop Service (CDS) commands in the OAM cds command group.

Table 71: OAM cds commands

Command	Description	Element Manager
`cdsShow`	Displays the current Converged Desktop configuration.	N/A
`cdsAgentShow`	Displays the Personal Call Assistance (PCA) information and status for an agent.	N/A

OAM elm commands: ELM module

The following table lists the OAM ELM module command in the OAM elm command group.

Table 72: OAM elm commands

Command	Description	Element Manager
`elmShow`	Displays a list of supported languages.	N/A
`elmRefresh`	Re-reads language list and locale files.	N/A

OAM emhelp commands: Element Manager help file related commands

The following table lists the OAM emhelp module command in the OAM emhelp command group.

Table 73: OAM emhelp commands

Command	Description	Element Manager
`unpackEmHelp`	Unpacks Element Manager help files.	N/A

OAM iset commands: iset module

The following table lists the OAM iset module commands in the OAM iset command group.

Table 74: OAM iset commands

Command	Description	Element Manager
`isetLocUpdate`	Update location information for a specified IP Phone.	N/A
`itgPLThreshold [xxx]`	Sets the gateway alarm packet threshold. Where: xxx = a number between 1 and 1000, and represents the threshold in 0.1% increments. The default value is 10 (1%). Packet loss which exceeds the threshold generates an SNMP trap and writes a message to the log file if logging is enabled.	N/A

Command	Description	Element Manager
`clearLockout [TN | IP]`	Clears the Virtual Office login or Branch User Config lockout for a particular IP Phone. Where: [TN | IP] = TN or IP address of an IP Phone	N/A
`dsetDelayHookswitchSet`	Sets the maximum time period in milliseconds that IP Phones wait for a hookswitch request.	N/A
`cookieShowByTN`	Displays the cookie list for an IP Phone specified by TN.	N/A
`cookieShowByName`	Displays the list of IP Phones with a particular cookie set.	N/A
`cookieRegShow`	Displays the cookie registry.	N/A
`isetSecGet ["[<IP>] [<Type>] [<TN>] [<Encryption>] [<Action>] [<DTLSCap>]"]`	Display signaling encryption related information about registered IP Phones, filtered by the specified query. Where: • <IP> = IP address of an IP Phone • <Type> = type of IP Phone (For example, 2004P2). • <TN> = terminal number of an IP Phone • <Encryption> = type of configured signaling encryption Where: - INSECURE = IP Phones that are not configured for signaling encryption - SECURE = IP Phones that are configured with USEC or DTLS signaling encryption - DTLS = IP Phones that are configured with DTLS signaling encryption - USEC = IP Phones that are configured with USEC (UNIStim Security) signaling encryption - ALL = IP Phones that are configured with any type of signaling encryption • <Action> = type of signaling protocol used by the IP Phone to communicate with the signaling server Where: - 1 = UNIStim	Y

Command	Description	Element Manager
	Note: If the target LTPS node has a “DTLS Best Effort” policy and the IP Phone is configured as DTLS-capable, the IP phone is switched to DTLS by the LTPS when it registers. - 6 = USEC (Secure UNIStim) All signaling messages, including registration messages, are protected by USEC. The LTPS detects IP phones that are using USEC and does not attempt to switch them to DTLS. - 7 = DTLS When a DTLS session is established, the IP Phone registers using UNIStim over DTLS. • <DTLSCap> = DTLS capability indicator Where: - YES = IP Phones that are DTLS-capable - NO = IP Phones that are DTLS-incapable - ALL = IP Phones that are DTLS-capable and IP Phones that are DTLS-incapable	
`isetSecShow`	Lists the IP Address, type, TN, configured signaling encryption, action byte, and DTLS capability for all registered IP Phones.	Y
`isetSecUpdateShow`	Display the result of the isetSecUpdate command. **Note:** Not available for CS 1000 Release 7.0 or later.	Y

OAM mam commands: MAM module

The following table lists the OAM MAM module commands in the OAM mam command group.

Table 75: OAM mam commands

Command	Description	Element Manager
`firmwareVersionShow`	Displays firmware version number.	Y
`IPInfoShow`	Displays information about an IP telephony node. • IP addresses for the ELAN and TLAN subnets • default router for the ELAN and TLAN subnets • subnet mask for the ELAN and TLAN subnets • IP routing table • IP configuration of the node	Y
`itgCardShow`	Displays Voice Gateway Media Card information.	Y
`itgMemShow`	Displays memory usage on the Voice Gateway Media Card.	Y
`resetOM`	Resets all operational measurement (OM) parameters collected after the last log dump, including:. • outgoing calls tried • outgoing calls completed • incoming calls tried • total voice time • total fax time • outgoing packets discarded • incoming packets out–of–sequence • average packet delay • average packet loss • number of Fallback-to-PSTN calls The parameters start from zero.	Y
`bootPFileGet ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]`	Updates the BOOTPtab file on the Voice Gateway Media Card with the BOOTPtab file on the specified host, account and path. The bootpFileGet task on the ITG host initiates an FTP session with the given parameters and downloads the file to flash file system.	N/A

Command	Description	Element Manager
`bootPFilePut ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]`	Sends the BOOTPtab file from the Voice Gateway Media Card to TM.	N/A
`configFileGet ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]`	Sends an updated CONFIG.INI file from TM to the Voice Gateway Media Card. Updates the CONFIG.INI file on the Voice Gateway Media Card with the CONFIG.INI file on the specified host, account, and path. The configFileGet task on the ITG host initiates an FTP session with the given parameters and downloads the file to flash file system. The CONFIG.INI file also contains the NRS IP address, gateway password, and gateway DN-port mapping table.	N/A
`omFilePut ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]`	Sends the current Operational Measurements (OM) file to the specified host.	N/A
`currOMFilePut ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]`	Sends the current Operational Measurements (OM) file to the specified host. The OMFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the Voice Gateway Media Card Operational Measurements file to the specified location on the host.	N/A
`prevOMFilePut ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]`	Sends the previous Operational Measurements (OM) file to the specified host. The OMFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the Voice Gateway Media Card Operational Measurements file to the specified location on the host.	N/A
`hostFileGet ["hostname"] ["username"] ["password"]`	Transfers any file from an FTP Server to the Voice Gateway Media Card. This command gets any file from the host and does a Get using FTP to the Voice Gateway Media Card.	N/A

Command	Description	Element Manager
["directory path"] ["filename"] ["ITGFileName"] [listener]	["ITGFileName"] = full path AND filename of where the file is to be placed. [listener] = indicates which module to inform of the successful file transfer. It can be set to –1 to be disabled.	
hostFilePut ["hostname"] ["username"] ["password"] ["directory path"] ["filename"] ["ITGFileName"]	Transfers any file from the Voice Gateway Media Card to an FTP Server.	N/A
swDownload ["hostname"] ["username"] ["password"] ["directory path"] ["filename"]	Loads a new version of software from the FTP host to the Voice Gateway Media Card. Updates the software on the Voice Gateway Media Card with the binary file received from an FTP server corresponding to the ["hostname"] IP address. The Voice Gateway Media Card FTP client performs a Get which downloads the file to the flash bank. A checksum is calculated to verify correct delivery. Once the new software version is successfully downloaded, the Voice Gateway Media Card must be rebooted with cardReset to run the new software. ["Hostname"] refers to either the IP address of the FTP host, the Voice Gateway Media Card itself, or another Voice Gateway Media Card, when a PC card in the /A: drive of the Voice Gateway Media Card contains the software binary file.	N/A
itgAlarmTest	Generates ITGxxxx test alarms.	Y
itgPLThreshold [xxx]	Sets the gateway alarm packet threshold. Where: xxx = a number between 1 and 1000, and represents the threshold in 0.1% increments. The default value is 10 (1%). Packet loss which exceeds the threshold generates an SNMP trap and writes a message to the log file if logging is enabled.	N/A
disiAll	Gracefully voice gateway service on the Signaling Server.	Y
enaAll	Enables voice gateway service on the Signaling Server.	Y

Command	Description	Element Manager
disServices	Causes the Voice Gateway Media Card or Signaling Server to gracefully switch the registered resources to the other Voice Gateway Media Cards or Signaling Servers located in the same node. This command does not interrupt established calls.	Y
enlServices	Enables all the Voice Gateway Media Cards or Signaling Servers to accept registrations of resources.	Y
servicesStatusShow	Displays the status of services (tps/iset/vtrk/gk).	Y
soCmdStatusShow	Displays the status of Service Switch-Over commands.	N/A
soHelpMenu	Displays all the commands that can be used for Services Switch-Over.	N/A
lossPlanPrt	Displays the offsets and current values for the handset, headset, and handsfree RLR and SLR.	Y

OAM ncs commands: Network Connection Service module

The following table lists the OAM Network Connection Service (NCS) module commands in the OAM ncs command group.

Table 76: OAM ncs commands

Command	Description	Element Manager
tpsARTrace IP [IP address] ID [User ID] ALL	Enables tracing for the Network Connection Server (NCS). Allows tracing of the tpsAR protocol, which is used to determine where an IP Phone should register. Where: • IP address = a string containing the IP Phone's IP address • User ID = the ID of the IP Phone to be traced (the DN used to log in) or the H323_Alias of where the IP Phone is trying to register • ALL = all IP Phones are to be monitored	N/A

Command	Description	Element Manager
`tpsARTraceOff IP [IP address] ID [User ID] ALL`	Disables tracing for the Network Connection Server (NCS). Removes the specified endpoint from the list of endpoints to be traced. Where: • IP address = a string containing the IP Phone's IP address • User ID = the ID of the IP Phone being traced (the DN used to log in) or the H323_Alias of where the IP Phone is =registered • ALL = removes monitoring of all IP Phones	N/A
`tpsARTraceAllOff`	Turns off the trace for all tpsAR trace identifiers.	N/A
`tpsAROutput [Output_Destination] ["File Pathname"]`	Modifies the destination for the traced output of the NCS. Sets the output for all tpsAR protocol traces. • [Output_Destination] = where all the trace messages for the tpsARTraceSet are to be directed The values are: - 1 = TTY - 2 = RPTLOG - 3 = File - 4 =TTY + File If the command is run from the OAM prompt or PDT prompt on the Signaling Server, then the values are the actual word, not a number: - TTY - RPTLOG - FILE - TTY + FILE • ["File Pathname"] = specifies the output file name if option 3 or 4 is selected.	N/A
`tpsARTraceSettings`	Displays the trace settings and items being traced for the NCS trace. Displays the trace tool settings, which endpoints are being traced, and where the trace output is being directed.	N/A
`tpsARTraceHelp`	Displays help on the tpsARTrace commands.	N/A

Command	Description	Element Manager
	Displays a list of all CLI commands used for tracing tpsAR protocol messages, including usage and parameters.	

OAM npm commands: Network Protocol Module

The following table lists the OAM Network Protocol Module (NPM) commands in the OAM npm command group.

Table 77: OAM npm commands

Command	Description	Element Manager
`H323GwRegTrace`	Turns the traces on and off for H.323 Registration at the gateway .	N/A
`H323CallTrace [ch] [channel #] [beginning channel #] [ending channel #] [num] [calling/called number] [NPI] [TON] [MsgRecv] [MsgSend]`	Traces H.323 incoming and outgoing call setup messages for selected channels or numbers. Traces a specified channel (ch) or number (num). Either the "ch" or "num" parameter must be specified (mutually exclusive). • [channel #] = a channel number Values range from 0 to the maximum channel number. • [beginning channel #] = the first channel number in a range of channel numbers. • [ending channel #] = the last channel number in a range of channel numbers. • [calling/called number] = a telephone number. The value can be a number from 1 to 32 digits and can be a partial "calling/called number". • [NPI] = a numbering plan identifier used to filter traces for a "calling/called number". The values are: - 0 - ALL - 1 - Unknown - 2 - ISDN/telephony numbering plan (E.164) - 4 - E.163 - 5 - Telex numbering plan (F.69) - 6 - Data numbering plan	N/A

Command	Description	Element Manager
	- 7 - National standard numbering plan • [TON] = the type of "calling/called number" number used to filter traces for a "calling/called number". The values are: - 0 - ALL - 1 - Unknown Number - 2 - International Number - 3 - National Number - 4 - Network Specific Number - 5 - Subscriber Number - 6 - Level 1 Regional - 7 - Level 0 Interface • [MsgRecv] specifies if the messages sent to the specified channel or calling/called number should be traced. The values are ON or OFF. • [MsgSend] specifies if the messages sent from the specified channel or calling/called number should be traced. The values are ON or OFF.	
`H323TraceShow`	Displays input and output display settings for **`H323CallTrace`** and **`H323Output`** commands. Displays the trace settings, including the output destination and filename, as well as all active traces for the H323CallTrace trace tool.	N/A
`H323Output [Output_Destination] ["File Pathname"]`	Directs H323Trace output to TTY or syslog file. Specifies where the output for the trace tool is to be directed. Where: • [Output_Destination] specifies where all the trace messages for H323CallTrace are to be directed. The values are: - 1 = TTY - 2 = RPTLOG - 3 = File	N/A

Command	Description	Element Manager
	- 4 = File and TTY • ["File Pathname"] specifies the file if option 3 or 4 is selected.	
`H323GwShow [ch] [channel #] [num] [calling/called number] [NPI] [TON]`	Displays information about the H.323 Network Protocol Module. Provides a general summary of the H.323 Virtual Trunk settings if no parameters are specified. Provides a general summary of the H.323 Virtual Trunk settings and a snapshot of the active call(s) for the specified channel(s), number(s), and trace filters, when the "ch" or "num" parameter is specified. When specified, the "ch" and "num" parameters are mutually exclusive. Where: • [channel #] = the channel number being traced Values range from 0 to maximum channel number • [calling/called number] indicates the telephone number to trace. The value can be a number from 1 to 32 digits and can be a partial "calling/called number". • [NPI] = the numbering plan identifier used to filter traces for a "calling/called number". The values are: - 0 - ALL - 1 - Unknown - 2 - ISDN/telephony numbering plan (E.164) - 4 - E.163 - 5 - Telex numbering plan (F.69) - 6 - Data numbering plan - 7 - National standard numbering plan • [TON] = the type of "calling/called number" number used to filter traces for a "calling/called number". The values are: - 0 - ALL - 1 - Unknown Number - 2 - International Number	N/A

Command	Description	Element Manager
	- 3 - National Number - 4 - Network Specific Number - 5 - Subscriber Number - 6 - Level 1 Regional - 7 - Level 0 Interface	

OAM nrsDB commands: Network Routing Service

The following table lists the OAM Network Routing Service (NRS) commands in the OAM nrsDB command group.

Table 78: OAM nrsDB commands

Command	Description	Element Manager
`nrsGWEndpointShow`	Lists all the NRS endpoints with corresponding IP addresses. Replaces the SIP proxy command gwshow.	N/A
`nrsUserEPShow`	Lists all the NRS users with corresponding IP addresses.	N/A
`nrsCollaboratingServerShow`	Lists all the Collaborating Servers in the database.	N/A
`nrsL0DomainShow`	Lists all the Level 0 regional domains in the database. Replaces the SIP proxy command l0dshow.	N/A
`nrsL1DomainShow`	Lists all the Level 1 regional domains in the database. Replaces the SIP proxy command l1dshow.	N/A
`nrsRoutingEntryShow`	Lists all the Routing Entries in the database. Replaces the SIP proxy command ryshow.	N/A
`nrsServiceDomainShow`	Lists all the Service Domains in the database. Replaces the SIP proxy command sdmshow.	N/A
`nrsCollaboratingServerQuery`	Queries one Collaborating Server from the database.	N/A
`nrsGWEndpointQuery`	Queries an NRS endpoint with IP and protocol information.	N/A

Command	Description	Element Manager
nrsUserEPQuery	Queries an NRS endpoint with IP and protocol information.	N/A
nrsL0DomainQuery	Queries a Level 0 regional domain with E164 information.	N/A
nrsL1DomainQuery	Queries a Level 1 regional domain.	N/A
nrsServiceDomainQuery	Queries one Service Domain from the database.	N/A
nrsDefaultRouteQuery	Queries an NRS default route. Displays all the default routes which belong to an endpoint in the database.	N/A
nrsDBShow	Displays the state of the Primary and Alternate NRS database, and the local NRS database.	N/A
nrsDBSyncForce	Forces synchronization of the active NRS database with the Alternate or Failsafe NRS database.	N/A
nrsDBStateShow	Displays the internal state in NRS DB.	N/A

OAM nrsomm commands: NRS operational measurements

The following table lists the OAM NRS operational measurements commands in the OAM nrsomm command group.

Table 79: OAM nrsomm commands

Command	Description	Element Manager
NrsOmmShow	Displays the SIP and H.323 NRS statistics for the current hour.	N/A
NrsOmmAvShow	Displays the SIP and H.323 NRS total statistics and average statistics for the last seven days.	N/A

OAM pbxlink commands: PBX link

The following table lists the OAM PBX link commands in the OAM pbxlink command group.

Table 80: OAM pbxlink commands

Command	Description	Element Manager
pbxLinkShow	Displays PBX link status. Displays information about the link to the CPU, including the configuration and link status.	Y

OAM securityShell commands: Security shell

The following table lists the OAM Security shell commands in the OAM securityShell command group.

Table 81: OAM securityShell commands

Command	Description	Element Manager
disInsecureShells	Disables all insecure shells in the system, including TELNET and RLOGIN sessions.	Y
enlInsecureShells	Enables all insecure shells in the system, including TELNET and RLOGIN sessions.	Y
statInsecureShells	Displays whether insecure shell access is enabled or disabled.	Y
disSecureShells	Disables all secure shells in the system, including SSH, SFTP, and SCP sessions. **Note:** You cannot disable SFTP and FTP sessions at the same time.	Y
enlSecureShells	Enables all secure shells, including SSH, SFTP, and SCP sessions.	Y
statSecureShells	Shows whether secure shell access is enabled or disabled.	Y

OAM sipcti commands: SIP CTI module commands

The following table lists the OAM sipcti commands in the OAM sipcti command group.

Table 82: OAM sipcti commands

Command	Description	Element Manager
`SIPCTISessionShow`	Shows the total number of TR87 SIP CTI sessions.	N/A
`SIPCTIClientShow`	Shows information about all the associated soft clients.	N/A
`SIPCTIShow`	Shows SIP CTI application status and configuration.	N/A
`SIPCTIStop [dn] [all]`	De-acquire one or all AST DN(s) and delete all associated TR87 SIP CTI sessions. Where: • [dn] = a specific AST DN • [all] = all AST DNs	N/A
`SIPCTITraceLevel [level]`	Sets the MessageTrace Level output to TR87 body only or Detailed format. [level] can be one of the following values: • 0 –TR87 SIP message body (ECMA 323) only • 1 – TR87 SIP message body (ECMA 323) and message headers	N/A
`SIPCTITraceShow`	Prints SIPCTI trace settings.	N/A
`SIPCTIOutput [Dest] ["filename"]`	Redirect the SIP CTI trace to a specific output destination. Where: • [Dest] = a specific output destination. The destination can be one of the following: - 1 TTY - 2 RPTLOG - 3 File • ["filename"] is specified only if option 3 (File) is specified.	N/A
`SIPCTITrace [sc] [soft client SIP/Tel URL/DN] [MsgRcv] [MsgSend]`	Trace incoming and outgoing TR87 SIP messages. Where: • [sc] parameter is not specified Turn on SIP CTI trace for all soft clients in incoming and/or outgoing directions. Where: - [MsgRcv] = On	N/A

Command	Description	Element Manager
	Trace all incoming SIP soft client messages. - [MsgRcv] = Off Do not trace all incoming SIP soft client messages. - [MsgSend] = On Trace all outgoing SIP soft client messages. - [MsgSend] = Off Do not trace all outgoing SIP soft client messages. • [sc] parameter is specified Turn on SIP CTI trace for a specific soft client in incoming and/or outgoing direction(s). Where: - [soft client SIP/Tel URL/DN] identifies the soft client for which calls are to be traced. This may result in a number of sessions as a single URL could be used for multiple active sessions. - [MsgRcv] = On Trace all incoming SIP soft client messages. - [MsgRcv] = Off Do not trace all incoming SIP soft client messages. - [MsgSend] = On Trace all outgoing SIP soft client messages. - [MsgSend] = Off Do not trace all outgoing SIP soft client messages.	
`SIPCTILdapForceUpdate`	Update LDAP cache from LDAP server.	N/A
`SIPCTILdapSetPageSize`	Set LDAP page size for LDAP caching.	N/A

OAM sipctiomm commands: SIP CTI OMM commands

The following table lists the OAM sipctiomm commands in the OAM sipctiomm command group.

Table 83: OAM sipctiomm commands

Command	Description	Element Manager
`SipCtiOmmShow`	Show the current hour count statistics for SIP CTI.	N/A

OAM sipnpm commands: SIP Network Protocol Module

The following table lists the OAM SIP Network Protocol Module commands in the OAM sipnpm command group.

Table 84: OAM sipnpm commands

Command	Description	Element Manager
`SIPGwShow <appName> [CH channel #] [NUM <calling/called number> [NPI] [TON]]`	Displays H.323 Virtual Trunk settings on the specified SIP GW application. Displays a summary of H.323 VTRK information, channel-related information (CH token), and number-related information (NUM token. If an optional command token and associated parameters are specified, the command provides a filtered snapshot of the active call(s) that match the token parameters, on the specified SIP GW application. When specified, the "CH" and "NUM" tokens and their associated parameters are mutually exclusive. Where: • <appName> = SIP gateway (GW) application - tSSG = Signaling Server SIP GW - tSLG = SIP Lines Server SIP GW • CH token parameters (channel-related message tracing): <channel #> = the channel number being traced Values range from 0 to maximum channel number. • NUM token parameters (number-related message tracing): - <calling/called number> = the telephone number to trace The value can be a number from 1 to 32 digits and can be a partial number.	Y

Command	Description	Element Manager
	- <NPI> = the numbering plan identifier used to filter traces for a "calling/called number" Allowable values: • 0 - ALL • 1 - Unknown • 2 - ISDN/telephony numbering plan (E.164) • 4 - E.163 • 5 - Telex numbering plan (F.69) • 6 - Data numbering plan • 7 - National standard numbering plan - <TON> = the type of number used to filter traces for a "calling/called number" Allowable values: • 0 - ALL • 1 - Unknown Number • 2 - International Number • 3 - National Number • 4 - Network Specific Number • 5 - Subscriber Number • 6 - Level 1 Regional • 7 - Level 0 Interface	
SIPCallTrace <appName> [(OFF)/ON] [CH <starting channel #> [<ending channel #>]] [NUM <calling/called number> [<NPI>] [<TON>]] <MsgRecv> <MsgSend>	Enable/disable SIP VTRK tracing, and initiate traces for SIP messages (active calls), on the specified SIP Gateway application. Supports tracing of all SIP messages, channel-related SIP messages (CH token), or number-related SIP messages (NUM token), in the receiving and/or sending directions. If an optional command token (CH or NUM) and associated parameters are specified, the command provides a filtered snapshot of the active call(s) that match the specified parameters within the appropriate context (token). When specified, the optional CH and NUM tokens and their associated parameters are mutually exclusive. Where: • <appName> = SIP gateway (GW) application - tSSG = Signaling Server SIP GW	N/A

Command	Description	Element Manager
	- tSLG = SIP Lines Server SIP GW • OFF = disable SIP VTRK tracing • ON = enable SIP VTRK tracing • CH token parameters (channel-related message tracing): - <starting channel #> = the number of a specific VTRK channel, or the starting number of a range of VTRK channels Values range from 0 to maximum channel number - 1. - <ending channel #> = the ending number of oa range of VTRK channels Values range from 1 to maximum channel number. • NUM token parameters (number-related message tracing): - <calling/called number> = the telephone number to trace The value can be a number from 1 to 32 digits and can be a partial number. - <NPI> = the numbering plan identifier used to filter traces for a "calling/called number" Allowable values: • 0 - ALL • 1 - Unknown • 2 - ISDN/telephony numbering plan (E.164) • 4 - E.163 • 5 - Telex numbering plan (F.69) • 6 - Data numbering plan • 7 - National standard numbering plan - [TON] = the type of number used to filter traces for a "calling/called number" Allowable values: • 0 - ALL • 1 - Unknown Number • 2 - International Number • 3 - National Number	

Command	Description	Element Manager
	• 4 - Network Specific Number • 5 - Subscriber Number • 6 - Level 1 Regional • 7 - Level 0 Interface • <MsgRecv> - specifies if incoming messages should be traced The values are ON or OFF. • <MsgSend> - specifies if outgoing messages should be traced The values are ON or OFF.	
`SIPTraceShow`	Displays the SIP trace settings and all active traces for the SIP call trace tool. Displays the output format, output destination and filename, as well as all active traces for the SIPCallTrace trace tool.	N/A
`SIPOutput [Output_Destination] ["File Pathname"]`	Specifies where the output for the SIPCallTrace command is to be directed. Where: • [Output_Destination] = the destination for all the trace messages output from the SIPCallTrace command. The values are: - 1 = TTY - 2 = RPTLOG - 3 = File - 4 = File and TTY • ["File Pathname"] specifies the file name if option 3 or 4 is selected.	N/A
`SIPTraceLevel <appname> <Output Option>`	Sets the SIPCallTrace output to Summary or Detailed format. Where: • <appname> = SIP gateway (GW) application - tSSG = Signaling Server SIP GW - tSLG = SIP Lines Server SIP GW • <Output Option> = the level of information to display - 0 = summary information - 1 = detailed information	N/A

Command	Description	Element Manager
SIPGwRegTrace <appName>	Turns the trace for SIP registration messages ON or OFF at the signaling gateway. Where: <appName> = SIP gateway (GW) application - tSSG = Signaling Server SIP GW - tSLG = SIP Lines Server SIP GW	N/A
slgShowUID <"userid">	Display detailed information for a given SIP Lines Gateway user (must be executed on the SIP Lines server).	N/A
slgSetShowAll	Display all registered clients on the SIP Lines Gateway (must be executed on the SIP Lines server).	N/A
slgShow	Display the status of the SIP Lines Gateway application (must be executed on the SIP Lines server).	N/A
slgTraceShow	Display the current trace filter on the SIP Lines Gateway (must be executed on the SIP Lines server).	N/A

OAM system commands: system administration commands

The following table lists the OAM system administration commands in the OAM system command group.

Table 85: OAM system commands

Command	Description	Element Manager
rudpShow		
routeShow	Displays the current host and network routing table.	Y
routeAdd ["Host/ Network IP address"] ["IP Gateway"]	Adds a route to the network routing table. The route is added to the host portion of the routing table.	Y
routeDelete ["IP Address"] ["IP Gateway"]	Deletes a route from the network routing table.	N/A

Command	Description	Element Manager
`ping ["host"] [numPackets]`	Tests that a remote host is reachable. This command sends an ICMP ECHO_REQUEST packet to a network host. The host matching the destination address in the packet responds to the request. If a response is not returned, the sender times out. This command is useful to determine if other hosts or Voice Gateway Media Cards are communicating with the sender card. Where: • ["host"] = the IP address of the network host to ping • [numPackets] = the number of ICMP ECHO_REQUEST packets to send If not specified, ping runs until it is stopped by Ctrl-C.	N/A
`who`	Displays all active User IDs and ports.	N/A
`arpShow`	Displays entries in the system ARP table.	N/A
`arpFlush`	Flushes all the entries in the system ARP table.	N/A
`diskSizeShow`	Displays the total physical size of the hard disk.	N/A
`memSizeShow`	Displays the total physical size of the memory.	N/A
`swVersionShow`	Displays software version.	Y
`date`	Displays the system date and time, and prompts to configure new system date and time.	N/A
`uptime`	Displays the amount of time lapsed since the last system reboot.	N/A
`stty [speed]`	Sets console speed. Where [speed] = baud rate for the console Available speeds are 9600, 19200, 38400, and 115200.	N/A
`consoleShow`	Displays console speed.	N/A
`ppp [option] [IP Address] [Options file path]`	Initiates a PPP connection with options. Where: • [option] = connection options Valid values for [option] are: - -l = signifies that the IP address is local Default IP address is 137.135.x.1. - -r = signifies that the IP address is remote	N/A

Command	Description	Element Manager
	Default IP address is 137.135.x.2. - -o = specifies the full path to the options file. - -f = specifies no hardware flow control signals during PPP connection. • [IP Address] = IP address where the PPP connection is initiated • [Options file path] = full path to the options file	
`sysResShow`	Displays the current usage of File Descriptors (FD) on the system.	N/A
`cppmLoopChange`	Changes the IPMG loop number location (CP PM Signaling Server only).	N/A
`cppmShelfChange`	Changes the IPMG shelf number location (CP PM Signaling Server only).	N/A
`cppmLocationShow`	Displays the loop and shelf location (CP PM Signaling Server only).	N/A

OAM tps commands: TPS module

The following table lists the OAM TPS module commands in the OAM tps command group.

Table 86: OAM tps commands

Command	Description	Element Manager
`disiTPS`	Gracefully disables the LTPS service on the Voice Gateway Media Card. Prevents new IP Phones registering on the card, and all registered IP Phones are redirected to another card when idle.	N/A
`enaTPS`	Enables the LTPS service.	N/A
`UKLossPlanSet`	Assigns UK-specific values to the loss plan of an IP Phone. Increases the Tx level of the IP Phone to match the requirement for the UK.	N/A
`lossPlanSet [transducer] [rlroffset] [slroffset]`	Adjusts the levels of a given transducer by the entered RLR and SLR offsets. Allows a variable offset from the default loss plan, to be entered for the specified transducer (handset, handsfree, or headset).	N/A

Command	Description	Element Manager
	Where: • [transducer] = the handset, handsfree, or headset for which the levels are to be adjusted • [rlroffset] = adjusts the level heard at the IP Phone. • [slroffset] = adjusts the level transmitted from the IP Phone. Positive numbers reduce the level (add loss). Negative numbers increase the level (add gain).	
`UKLossPlanClr`	Removes the loss plan adjustments and returns the IP Phone to the default loss plan levels.	N/A
`lossPlanClr`	Removes the loss plan adjustments and returns the IP Phone to the default loss plan levels.	N/A

OAM trace commands: General trace tools

The following table lists the OAM General trace tools in the OAM trace command group.

Table 87: OAM trace commands

Command	Description	Element Manager
`traceAllOff`	Disables the trace facilities from writing to the TTY, SYSLOG, and specified files. Causes all traces that use the monitorLib server to stop their output. This is a temporary disabling function.	N/A
`traceAllOn`	Enables the trace facilities to resume writing to the TTY, SYSLOG, and/or specified files. Clears the blocking of all trace information imposed on the monitorLib service by the traceAllOff, tracePrintOff, and traceFileOff commands. By default, all tracing is on.	N/A
`tracePrintOff`	Disables the trace facilities from writing to the TTY. Blocks all logging of information received by the monitorLib service to the TTY output. This does not include traces directed through the monitorLib service to the RPT.LOG or SYSLOG.n services.	N/A
`tracePrintOn`	Enables the trace facilities to resume writing to the TTY.	N/A

Command	Description	Element Manager
	Clears only the TTY output blocking that was imposed by the traceAllOff and tracePrintOff commands.	
`traceFileOff`	Disables the trace facilities from writing to the SYSLOG and specified files. Causes the monitorLib server to stop logging to the log files any and all trace information received by the service. The log files include syslog.n for the Voice Gateway Media Card and rpt.log for the Signaling Server.	N/A
`traceFileOn`	Enables the trace facilities to resume writing to the SYSLOG and/or specified files. Clears only the blocking of logging to files that was imposed by the traceAllOff and traceFileOff commands.	N/A
`traceShow`	Displays the names of active traces in the system.	N/A

OAM uipc commands: Universal ISDN Protocol module

The following table lists the OAM Universal ISDN Protocol module commands in the OAM uipc command group.

Table 88: OAM uipc commands

Command	Description	Element Manager
`DCHmenu`	Displays a menu of DCH diagnostic tools. Displays a menu to perform various information retrieval operations for the D-channel. **`oam>DCHmenu`** Please select one of the DCHmenu options: • 0 - Print menu (default) • 1 - Print current DCH state • 2 - Print current DCH configuration • 3 - Print application error log • 4 - Print link error log • 5 - Print protocol error log • 6 - Print message log	N/A

Command	Description	Element Manager
	• 7 - Enable printing all messages processed by UIPC • 8 - Enable error printing • 9 - Enable info printing • 10 - Enter manual message mode • 11 - Print b channel control blocks • 99 - Exit menu	

OAM ums commands: UMS module

The following table lists the OAM UMS module commands in the OAM ums command group.

Table 89: OAM ums commands

Command	Description	Element Manager
`umsPolicyshow`		
`firmwareFileGet ["ServerIP"] ["UserID"] ["Password"] ["/path/to/file"] ["Filename"]`	Initiates a firmware download from a specified FTP server. After the download is completed, the downloaded file is checked for Enhanced Header (or proper naming). If the file is considered a valid firmware file, the UMS database is updated accordingly. Where: • ["ServerIP"] – FTP server IP address from where the firmware will be retrieved • ["UserID"], ["Password"] – credentials for logging into the FTP server • ["/path/to/file"] – absolute or relative path to the firmware file (does not include the file name itself) • ["Filename"] – name of the firmware file on the FTP server Use the **`firmwareFileGet`** command instead of the **`firmwareFileGetI2004`**, **`firmwareFileGetI2002`**, and **`firmwareFileGetIPP2`** commands.	N/A

Command	Description	Element Manager
`firmwareFileGetI2004`	Initiates a firmware download for an IP Phone 2004 from a specified FTP server. Replaced by **`firmwareFileGet`**.	N/A
`firmwareFileGetI2002`	Initiates a firmware download for an IP Phone 2002 from a specified FTP server. Replaced by **`firmwareFileGet`**.	N/A
`umsUpgradeAll ["hh:mmx"]`	Upgrades all registered sets according to policy and firmware file. Where: • hh:mm = specifies the time when the upgrade will occur • x = specifies whether the time is AM or PM - a = AM - p = PM **Caution:** If the umsUpgradeAll command is used without the time parameter, all IP Phones registered on cards that are logged into are immediately taken out of service. Use the time parameter with the command to prevent this from happening.	N/A
`umsUpgradeTimerShow`	Displays the upgrade schedule.	N/A
`umsUpgradeTimerCancel`	Cancels the scheduled upgrade.	N/A

OAM usi commands: RUDP timeout and retry commands

The following table lists the OAM RUDP timeout and retry commands in the OAM usi command group.

Table 90: OAM usi commands

Command	Description	Element Manager
`usiSetPhoneRudpRetries`	Configures the RUDP Max Retries count for IP Phones.	N/A
`usiGetPhoneRudpRetries`	Displays the RUDP Max Retries count for IP Phones.	N/A

Command	Description	Element Manager
`usiSetPhoneRudpTimeout`	Configures the RUDP Timeout value (in milliseconds) for IP Phones.	N/A
`usiGetPhoneRudpTimeout`	Displays the RUDP Timeout value (in milliseconds) for IP Phones.	N/A

OAM vte commands: Virtual Terminal Emulator

The following table lists the OAM Virtual Terminal Emulator commands in the OAM vte command group.

Table 91: OAM vte commands

Command	Description	Element Manager
`unpackVTHelp`	Unpacks Virtual Terminal Emulator help files.	N/A

OAM vtrk commands: Virtual Trunk module

The following table lists the OAM Virtual Trunk module commands in the OAM vtrk command group.

Table 92: OAM vtrk commands

Command	Description	Element Manager
`vtrkShow [<protocol>] [<start#>] [<howMany>]`	Display information about the Virtual Trunk (VTRK) channels for a particular signaling protocol. Where: • [protocol] = VTRK protocol - SIP = SIP protocol - H323 = H.323 protocol - SIPL = SIP Lines protocol If <protocol> is not specified, the command displays a summary of all VTRK protocols. • <start#> = the channel number at which to start the trunk summary display	Y

Command	Description	Element Manager
	If <start#> is not specified, the display starts from the first channel of the implicated protocol(s). • <howMany> = the number of trunk channels to be displayed If <howMany> is not specified, the command displays all trunk channels for the implicated protocol(s), starting from the channel ID specified in <start#>.	
`disVTRK`	Gracefully switches the registered Virtual Trunks to another Signaling Server in the same node. **Note:** LTPS and VTRK functions must be enabled on a Signaling Server located in the same node to accept VTRK registrations. The number of VTRK resources available must be equal to or greater than the number of VTRK resources being switched over.	Y
`forcedisVTRK`	Forces all registered Virtual Trunks to unregister from the local server.	Y
`enlVTRK`	Enables the Virtual Trunk application to accept Virtual Trunk registrations.	Y
`vtrkNetMonShow`	Display the current list of monitored IP addresses and their status.	N/A

OAM cds commands: Converged Desktop Service module commands

The following table lists the OAM cds module commands in the OAM cds command group.

Table 93: OAM cds commands

Command	Description	Element Manager
`amlAcquiredTNShow <"TN">`	Displays the contents of the Acquired DN List table for a specified TN. Where <TN> = terminal number in quotations (for example, "4 0 1 0" If DNs of the given <TN> are acquired by one or more application links, the output is as follows: `The DN1 of the <TN> is acquired by: <Application ID1>`	N/A

Command	Description	Element Manager

	`<Application ID2>`
	
	`The DN2 of the <TN> is acquired by:`
	`<Application ID1>`
	`<Application ID2>`
	
	If no DNs of the given <TN> are acquired by any application, then the following is displayed:
	
	`The TN <TN> is not acquired by any application through the AML FE.`	

`amlApplLinkShow [<Application ID>]`	Displays the record in the Application Link Table with the given <Application ID>.
	Where <Application ID> identifies a specific application.
	If there is a record in the Application Link Table with the given <Application ID>, then the following is displayed:
	
	`<Application ID>`
	`IP Address: ###.###.###.###`
	`Message Filter Bitmap:  0X##(in Hex)`
	`Feature Control Bitmap: 0X##(in Hex)`
	`Number of Acquired DNs: ####`
	
	If there is no record in the Application Link Table with the given <Application ID>, then the following is displayed:
	
	`No record for an application link with the given Application ID.`
	
	Note:
	If no <Application ID> is specified, all records (up to 5) in the Application Link Table are displayed.
		N/A

`amlAcquiredTNClearAll`	Clear the “Acquired TN Table”, all the “Acquired DN Lists” and their related “Application ID Lists”, and update the “Application Link Table” accordingly. The "acquired" resources on the CS are not de-acquired by this command. The command DACR ALL <AML Link Number for the AML FE> should be issued in LD 48 on the CS to de-acquire all the resources acquired through the AML FE.	N/A

Command	Description	Element Manager

	For example, if at least one IP Phone is acquired by at least one application, the output of this command is:
	`OK. Please issue command "DACR ALL #" in the overlay 48 on the CS.`
	If no IP Phones are acquired by any applications, the output of this command is:
	`No phone is acquired through the AML FE.`	

Level Two (PDT) CLI commands

This section lists the CLI commands that are only available (visible, executable) in the Level Two (Problem Determination Tool [PDT]) security shell.

All Level One OAM security shell CLI commands are available in the Level Two PDT security shell by default; PDT security shell capabilities are inclusive of all OAM security shell capabilities. For that reason, the OAM security shell CLI commands are not repeated in this section. To view Level One OAM security shell CLI commands, see Level One (OAM) CLI commands on page 601.

Some of the CLI commands that are only available in the PDT security shell are grouped into Command Groups that are also only available in the PDT security shell. However, some of the CLI commands that are only available in the PDT security shell, reside in Command Groups that span both the OAM and PDT security shells. In this section, the tables for the Command Groups that span both the OAM and PDT security shells contain the CLI commands that are only available in the PDT security shell. To obtain a full list of CLI commands in one of these Command Groups, you must look at the applicable Command Group tables in both the Level One OAM CLI Commands section and this section.

To display a list of the Command Groups available in the PDT security shell, type **`help`** at the PDT security shell command prompt (**`pdt>`**). To display a list of commands in a PDT security shell Command Group, type **`help <command group name>`** at the PDT security shell command prompt.

PDT Command groups

The following table lists the Command Groups available in the PDT security shell. Those Command Groups available only in the PDT security shell are in italics. The other Command Groups are available in the OAM security shell, but contain commands available only in the PDT security shell.

Table 94: PDT CLI command groups

Command group	Description	PDT Commands
Accounts	User account administration.	Table 95: Accounts commands on page 647
PDT	PDT built-in commands	Table 96: PDT built-in commands on page 648
Patcher	Patch commands	Table 97: PDT Patcher commands on page 648
RID	Remote iset diagnostics commands	Table 98: PDT RID commands on page 650
cds	Converged Desktop Service Module commands	Table 99: PDT cds commands on page 650
disk	File system maintenance and diagnostics.	Table 100: disk commands on page 652
nrsDB	Network Routing Service commands	Table 101: PDT nrsDB commands on page 652
rdtools	rd tools commands	Table 103: PDT rdtools commands on page 655
sipnpm	SIP Network Control Module commands	Table 104: PDT sipnpm commands on page 656
system	System administration commands	Table 105: PDT system commands on page 658
ums	UMS module commands	Table 106: PDT ums commands on page 660
iset	iset module commands	Table 107: PDT iset commands on page 661

PDT Commands

The following tables list the commands in each Command Group at the PDT access level. To display a list of commands in a specific PDT Command Group, type **help <command group name>** at the prompt.

Accounts commands: user account administration commands

The following table lists the user account administration commands in the Accounts command group.

Table 95: Accounts commands

Command	Description	Element Manager
adminUserPassword Change [userID]	Changes the administrator-level user password for an NRS running on a stand-alone Signaling Server. Where: userID = userID of administrator-level user	N/A
adminUserCreate [userID]	Creates an administrator-level user of an NRS running on a Standalone Signaling Server. Where: userID = userID of new administrator-level user	N/A
adminUserDelete [userID]	Deletes an administrator-level user of an NRS running on a Standalone Signaling Server. Where: userID = userID of administrator-level user being deleted	N/A
adminAccountShow	Displays User ID and access privileges for all users of an NRS running on a Standalone Signaling Server.	N/A

PDT built-in commands: PDT built-in

The following table lists the PDT built-in commands in the PDT command group.

Table 96: PDT built-in commands

Command	Description	Element Manager
`vxshell`	Switch user.	N/A
`vxWorksShell`	Switch user.	N/A

PDT Patcher commands: patcher

The following table lists the PDT patcher commands in the PDT Patcher command group. These commands are in addition to the OAM Patcher commands listed in Table 68: OAM Patcher commands on page 612

Table 97: PDT Patcher commands

Command	Description	Element Manager
`pload ["patch-filename"]`	Loads a patch file from the file system in Flash memory into DRAM memory, where [patch-filename] is the filename or path of the patch file. If a filename alone is provided, the patch must be in the /C:/u/patch directory. Otherwise, the full or relative path can be provided. When a patch is successfully loaded, the command returns a patch handle number. The patch handle number is used as input to other patch commands (pins, poos, pout, and plis). The loaded patch is inactive until it is put into service using the pins command. If the command is issued without a parameter, you are prompted for the patch filename and other information.	N/A
`pins [handle]`	Puts a patch that has been loaded into memory (using the pload command) into service, where [handle] is the number returned by the pload command. If the command is issued without a parameter, you are prompted to enter a [handle]. If issued successfully, the command indicates the global procedures, functions, or areas of memory affected by the patch. You are then prompted and have the choice to proceed or not to proceed.	N/A
`poos [handle]`	Deactivates a patch (takes it out-of-service) by restoring the patched procedure to its original state.	N/A

Command	Description	Element Manager
	If the poos command is issued without a parameter, you are prompted to enter a [handle].	
`pout [handle]`	Removes a patch from DRAM memory. The patch must be taken out-of-service (using the poos command) before it can be removed from the system. If the pout command is issued without a parameter, you are prompted to enter a handle.	N/A
`plis [handle]`	Lists detailed patch status information for a loaded patch. If the command is issued without a parameter, you are prompted to enter a [handle].	N/A
`pstat [handle]`	Displays summary status information for one or all loaded patches. For each patch, the following information is displayed: patch handle, filename, reference number, whether the patch is in-service or out-of-service, the reason why the patch is out-of-service (if applicable), and whether the patch is marked for retention or not. Patch retention means that if a reset occurs, then the patch is automatically reloaded into memory and its state (active or inactive) is restored to what it was prior to the system going down. If the [handle] is provided, only the information for the specified patch is displayed. If the command is issued without a parameter, information for all the patches is displayed.	N/A
`pnew`	Creates memory patches for the Media Gateway Card. The command has no parameter(s). The release of the patch is assumed to be the same as that of the current load. The address to be patched is checked to ensure that it is in range. For each address that is changed, the "old" contents are assumed to be the current contents of that memory address. If a path is not provided for the new path filename then it is assumed that the patch is in the /C:/u/ patch directory. Once a memory patch is created using the pnew command, it can be loaded and activated like any other patch.	N/A
`dload`	Loads one or all deplists.	N/A

Command	Description	Element Manager
dins	Activates one or all deplists.	N/A
dstat	Displays the status of the requested deplist or all deplists.	N/A
dlis	Displays a summary of the status of all patches in a deplist.	N/A
doos	Deactivate one or all deplists.	N/A
dout	Remove one or all deplists from memory.	N/A

PDT RID commands: remote iset diagnostics

The following table lists the PDT remote iset diagnostic commands in the PDT RID command group.

Table 98: PDT RID commands

Command	Description	Element Manager
RTPTraceShow	Displays RTCP statistics periodically for an IP Phone for a number of polling periods.	N/A
RTPTraceStop	Stops previously issued RTPTraceShow command for an IP Phone.	N/A

PDT cds commands: Converged Desktop Service module

The following table lists the PDT Converged Desktop Service module commands in the PDT cds command group. These commands are in addition to the OAM cds commands listed in Table 71: OAM cds commands on page 614

Table 99: PDT cds commands

Command	Description	Element Manager
cdsCallTraceSetDN	Enables CDS call tracing for a particular calling/called DN.	N/A
cdsCallTraceSetAll	Enables CDS call tracing for all converged desktop calls.	N/A

Command	Description	Element Manager
cdsCallTraceOff	Turns off CDS call tracing for all converged desktop calls.	N/A
cdsAmlTrace	Turns off AML message tracing for Converged Desktop Service module.	N/A
amlTrace <Level Number> <AML over PBXlink_On/OFF> [<Application ID List>]	Enables tracing of AML messages between the call server and the AML FE on the signaling server, with or without decoding. Where: • <Level Number> = integer defining the display level for AML messages Where: - 1 = raw AML link messages, no decoding - 2 = raw AML messages, excluding polling messages, with no decoding - 3 = decoded AML messages, exluding decoding of IE data - 4 = decoded AML messages, including decoded IE data • integer indicating whether to turn on or turn off tracing of AML messages arriving at the PBXLink Where: - 0 = turns off AML tracing - 1 = turn on AML tracing • <Application ID List> = a set of integers indicating specific applications for which related AML messages are traced If no value(s) are specified, AML messages from all applications are traced.	

amlTraceShow	Displays current status (settings) of amlTrace command when the AML trace is ON.
	`Trace Level: #`
	`AML over PBXLink: #`
	`Assigned Application IDs: ##, ##`
	When AML trace is OFF, the following information is displayed:
	`AML Trace is Off`
		N/A

disk commands: file system maintenance and diagnostics

The following table lists the PDT file system maintenance and diagnostic commands in the disk command group.

Table 100: disk commands

Command	Description	Element Manager
`fsck [m] [devname]`	Checks the integrity of the file system on the specified device. Errors are repaired unless the mount flag is specified. Where: • [m] is the mount flag • [devname] is the device to check	N/A

PDT nrsDB commands: Network Routing Service

The following table lists the PDT Network Routing Service (NRS) commands in the nrsDB command group. These commands are in addition to the OAM nrsDB commands listed in Table 78: OAM nrsDB commands on page 626.

Table 101: PDT nrsDB commands

Command	Description	Element Manager
`nrsDBCutover`	Switches the active and standby NRS database access pointer.	N/A
`nrsDBRevert`	Reverses the effect of the nrsDBCutever command.	N/A
`nrsDBCommit`	Mirrors data from the active NRS database to the standby NRS database.	N/A
`nrsDBRollback`	Undoes the changes effected by the nrsDBCutover and nrsDBCommit commands, whether executed seperately, or as one (nrsDBCommitNow).	N/A
`nrsDBCommitNow`	Performs the nrsDBCutover command and the nrsDBCommit command respectively, as one.	N/A
`disNRS`	Gracefully disables the NRS server.	N/A

Command	Description	Element Manager
	Note: This command should not interrupt the existing calls.	
forcedisNRS	Forcefully disables the NRS server (puts the NRS server out-of-service).	N/A
enlNRS	Enables the SIP Redirect Server service.	N/A
nrsGKTestQuery	Test query the H.323 routes on the active or standby NRS database. Queries an H.323 Routing Entry with DN and cost information.	N/A
nrsSIPTestQuery	Test query the SIP routes on the active or standby status NRS database. Queries a SIP Routing Entry with DN and cost information.	N/A
spcmd	Database operations and applications log	N/A
isetResetByS1 <soft | hard>	Reset all sets which are registered through S1. This command is going through the list of sets registered and performs hard or soft reset (based on parameter given) of sets which are registered through S1.	N/A
isetresetByS2 <soft | hard>	Reset all sets which are registered through S1. This command is going through the list of sets registered and performs hard or soft reset (based on parameter given) of sets which are registered through S2.	N/A
isetSwitchToS1	Switch all sets which are registered through S2 to S1. This command is going through the list of sets registered and performs server switch to S1 sets which are registered through S2.	N/A
isetSwitchToS2	Switch all sets which are registered through S1 to S2. This command is going through the list of sets registered and performs server switch to S2 sets which are registered through S1.	N/A
isetResetLocal	Reset all sets which are in local mode. This command is going through the list of sets registered and performs soft reset of sets which are currently in local mode.	N/A
isetResetNormal	Reset all sets which are in normal mode. This command is going through the list of sets	N/A

Command	Description	Element Manager
	registered and performs soft reset of sets which are currently in normal mode.	
isetResetVO	Reset all sets which are in VO mode. This command is going through the list of sets registered and performs soft reset of sets which are currently in virtual office mode.	N/A

Note:
The database cutover, revert, commit, and rollback commands are not available in the Element Manager user interface. The same functionality is available in NRS Manager at **Tools > Database Actions**.

The spcmd command can be used for various operations. The syntax of the SIP Proxy spcmd command is:

Usage: spcmd [cmd family][parameter <value> ...]

Table 102: spcmd Command description

Family	Parameter	Description
-D	-d failsafe	
-L	-v debug | info | all	Write debug, info, or all (i.e. both) logs in addition to the sipLogFile.
	-s on | off	Turn on/off the log types listed by the -v parameter. If no parameter is given, the default is set to on. Default is on.
-O	-v 400 | 401 | 407 | hw | ss	Display OM report for 400, 401, 407, or 3XX responses as well as the high water (hw) mark for internal queue memory usage and the number of SIP sessions (ss) that have been established.
-R	-s force | wait | now -t now | 1..99 -u min | sec	Execute a shutdown and restart of the application immediately or in some given time unit (min\sec) whether call are executing or not by either forcing the application or waiting for call processing to stop.
-S	-s force | wait -t now | 1..99 -u min | sec	Execute a switching of activity from the running application processing to stop where a timer value can be given.

Family	Parameter	Description
-V	-v app | stack | all	Show the version of the application, oSIP stack, or both.

rdtools commands: rd tools

The following table lists the PDT rd tools commands in the PDT rdtools command group.

Table 103: PDT rdtools commands

Command	Description	Element Manager
`rdopen [filename]`	Opens a report log file. Where: [filename] is the name of the report file to be opened.	N/A
`rdgo [N]`	Goes to a specific record. Where: [N] is the absolute record number.	N/A
`rd [S] [R]`	Displays a specified number of records starting at a specified point. Where: • [S] is the number of steps to traverse to the starting point. • [R] is the number of records to display. Both [S] and [R] can be negative.	N/A
`rds [S] [R]`	Displays a specified number of records, with a symbolic dump, starting at a specified point. Where: • [S] is the number of steps to traverse to the starting point. • [R] is the number of records to display. Both [S] and [R] can be negative.	N/A
`rdshow`	Displays general information about the current log file and the current rd settings.	N/A
`rdall`	Displays all records.	N/A
`rdtail [N]`	Displays the specified number of newest records.	N/A

Command	Description	Element Manager
	Where: [N] is the number of records to display.	
`rdhead [N]`	Displays the specified number of oldest records. Where: [N] is the number of records to display.	N/A
`rdnext`	Opens the next log file.	N/A
`rdprev`	Opens the previous log file.	N/A
`rdsconvert [filename]`	Converts a log file to text. Where: [filename] is the name of the log file to be converted.	N/A

PDT sipnpm commands: SIP Network Protocol Module

The following table lists the PDT SIP Network Protocol Module commands in the sipnpm command group that are available only at the PDT access level. These commands are in addition to the OAM sipnpm commands listed in Table 84: OAM sipnpm commands on page 631.

Table 104: PDT sipnpm commands

Command	Description	Element Manager
`SIPTLSConfigShow`	Displays the details of the TLS parameters. Displays TLS configuration parameters for the system as a whole, including client and server session caching parameters, the certificate for the local system, and the certificates that are configured.	N/A
`SIPTLSSessionShow`	Displays the details of the TLS sessions. Displays the details of all SIP TLS sessions or sessions associated with a given server IP address. Displays existing sessions (in connected state and persistent), cached sessions, and the uptime and cipher suites, but does not show key information.	N/A
`SIPMessageTrace`	Configures filtering criteria for message tracing.	N/A

Command	Description	Element Manager
`sip2IsdnSet [num1] [num2]`	Changes the SIP status code to the ISDN cause code mapping. Where: • [num1] = the SIP status code • [num2] = the ISDN cause code	N/A
`sip2IsdnReset [num]`	Resets a single SIP status code to the default ISDN cause code mapping. Where: [num] = the SIP status code.	N/A
`sip2IsdnResetAll`	Resets all SIP status codes to the default ISDN cause code mappings.	N/A
`sip2IsdnShow [num]`	Shows one specific SIP status code to ISDN cause code mapping. Where: [num] = the ISDN cause code.	N/A
`sip2IsdnShowAll`	Shows all mappings from SIP status code to ISDN cause code.	N/A
`isdn2SipSet [num1] [num2]`	Changes the ISDN cause code to the SIP status code mapping. Where: • [num1] = the ISDN cause code • [num2] = the SIP status code	N/A
`isdn2SipReset [num]`	Resets a single ISDN cause code to the default SIP status code mapping. Where: [num] = the ISDN cause code.	N/A
`isdn2SipResetAll`	Resets all the ISDN cause codes to the default SIP status code mappings.	N/A
`isdn2SipShow [num]`	Shows one specific ISDN cause code to SIP status code mapping. Where: [num] = the ISDN cause code.	N/A
`isdn2SipShowAll`	Shows all mappings from ISDN cause codes to SIP status codes.	N/A

PDT system commands: System administration

The following table lists the system administration commands in the system command group that are available only at the PDT access level. These commands are in addition to the OAM system commands listed in Table 85: OAM system commands on page 635.

Table 105: PDT system commands

Command	Description	Element Manager
`lkup`	Look up a symbol.	N/A
`devs`	Displays list of the devices.	N/A
`echo`	Echoes the input.	N/A
`hosts`	Displays a list of hosts.	Y
`memShow`	Displays memory usage.	Y
`ti [name | taskID]`	Displays task information for a specified task. Where: • [name] is the name of the task. • [taskID] is the ID of the task. [name] and [taskID] are mutually exclusive.	N/A
`i`	Displays a summary of task control block information.	System
`version`	Displays vxWorks™ version, date of build, and other information.	Y
`x [name]`	Executes a function. Where: [name] = the name of the function.	N/A
`ifShow`	Displays the attached network interfaces.	Y
`reboot [-1]`	Warm reboots the system. Cold reboots the system if the -1 parameter is specified.	N/A
`ls [path]`	Displays the contents of a directory. Where: [path] = the path name of the directory. If [path] is not specified, the contents of the current directory are displayed.	N/A

Command	Description	Element Manager
`ll [path]`	Displays a long list of the contents of a directory. Where: [path] = the path name of the directory. If path is not specified, the contents of the current directory are displayed.	N/A
`cd [path]`	Changes the default directory. Where: [path] = the path and name of the new directory. The [path] of the new directory can be specified as a relative path.	N/A
`pwd`	Displays the current default directory.	N/A
`copy [input] [output]`	Copies from one file to another file until an end-of-file (CTRL+d) is reached. Where: • [input] = the name of the file to be copied from. If NULL, stdin is used. • [output] is the name of the new or destination file to be copied to. If NULL, stdout is used.	N/A
`rename [file1] [file2]`	Renames one file or moves one file to another. Where: • [file1] = the file to be renamed or moved. • [file2] = the new or destination filename.	N/A
`remove [file]`	Removes a file. Where: [file] = the name of the file to be removed.	N/A
`moduleShow`	Displays the list of all loaded modules.	N/A
`inetstatShow`	Displays all the active connections for the IP sockets.	N/A
`tcpstatShow`	Displays statistics for the TCP protocol.	N/A
`udpstatShow`	Displays statistics for the UDP protocol.	N/A
`syslogShow`	Displays the log level for all tasks.	N/A

Command	Description	Element Manager
`syslogLevelSet [tid] [name] [level]`	Configures the log level for a task. Where: • [tid] = the task ID. • [name] = the task name. • [level] = the log level in the range 0-7. [tid] and [name] are mutually exclusive.	N/A
`uudecode`	Decode data that were encoded with `uuencode`	N/A
`arpPrivLogDisable`	Disable the Arp Warning messages report (when ELAN and TLAN are not isolated).	N/A
`arpPrivLogEnable`	Enable the Arp Warning messages report.	N/A
`hwdShow`	Displays the status of the system hardware watchdog timer.	N/A

PDT ums commands : UMS module commands

The following table lists the UMS module commands in the ums command group that are available only at the PDT access level. These commands are in addition to the OAM ums commands listed in Table 89: OAM ums commands on page 640

Table 106: PDT ums commands

Command	Description	Element Manager
`umsSetPolicy`	Assigns the policy for the particular firmware.	N/A
`umsSetPolicyUpgradeType`	Set upgrade type for policy.	N/A
`umsSetPolicyRetries`	Sets the number of retries for the policy.	N/A
`umsSetPolicyProtocol`	Sets the protocol for the policy.	N/A
`umsCreatePolicy`	Creates a firmware policy.	N/A
`umsDeletePolicy`	Deletes a firmware policy.	N/A

PDT iset commands: iset module commands

The following table lists the iset module commands in the iset command group that are available only at the PDT access level. These commands are in addition to the OAM iset commands listed in Table 74: OAM iset commands on page 615.

Table 107: PDT iset commands

Command	Description	Element Manager
`isetSecUpdate ["[<IP>] [<Type>] [<TN>] [<Encryption>] [<Action>] [<DTLSCap>]"] <ServerID> <Action> [<port>]`	Re-configure S1/S2 ports and action bytes on the targeted IP Phones. The first 6 parameters are used to specify the "target" IP Phones. Where: • <IP> = IP address of an IP Phone • <Type> = type of IP Phone (For example, 2004P2). • <TN> = terminal number of an IP Phone • <Encryption> = type of configured signaling encryption Where: - INSECURE = IP Phones that are not configured for signaling encryption - SECURE = IP Phones that are configured with USEC or DTLS signaling encryption - DTLS = IP Phones that are configured with DTLS signaling encryption - USEC = IP Phones that are configured with USEC (UNIStim Security) signaling encryption - ALL = IP Phones that are configured with any type of signaling encryption • <Action> = type of signaling protocol used by the IP Phone to communicate with the signaling server Where: - 1 = UNIStim **Note:** If the target LTPS node has a “DTLS Best Effort” policy and the IP Phone is configured as DTLS-capable, the IP phone	N/A

Command	Description	Element Manager
	is switched to DTLS by the LTPS when it registers. - 6 = USEC (Secure UNIStim) All signaling messages, including registration messages, are protected by USEC. The LTPS detects IP phones that are using USEC and does not attempt to switch them to DTLS. - 7 = DTLS When a DTLS session is established, the IP Phone registers using UNIStim over DTLS. • <DTLSCap> = DTLS capability indicator Where: - YES = IP Phones that are DTLS-capable - NO = IP Phones that are DTLS-incapable - ALL = IP Phones that are DTLS-capable and IP Phones that are DTLS-incapable • <ServerID> = indicates the server setting to be updated on the targeted IP Phones Where: - 1 = S1 setting - 2 = S2 setting • <Action> = the type of signaling protocol to be configured on the targeted IP Phones Where: - 1 = UNIStim **Note:** If the target LTPS node has a “DTLS Best Effort” policy and the IP Phone is configured as DTLS-capable, the IP phone is switched to DTLS by the LTPS when it registers. - 6 = USEC (Secure UNIStim) All signaling messages, including registration messages, are protected by USEC. The LTPS detects IP phones that are using USEC and does not attempt to switch them to DTLS. - 7 = DTLS	

Command	Description	Element Manager
	IP Phone registers using UNIStim over DTLS. • <Port> = the port number to be configured on the targeted IP Phones Default port number is 4100 if <Action> is set to 1 or 6. Default port number is 4101 if Action is set to 7. **Note:** Avaya does not recommend specifying an explicit port number unless there is a need to do so. **Note:** The configuration settings applied by this command will only be in effect if the targeted IP Phones are configured statically. If DHCP or a Provisioning Server is used to supply S1 and S2 configuration to the phones, the corresponding configuration source has to be updated instead of the IP Phones. Reboot of updated IP phones is required for configuration changes to take effect.	

CLI commands in Linux

This section lists CLI commands that are not supported in CS1000 Release 6.0 Linux.

Commands	Description
isecChgPSK isecChgLevel isecNewTarget isecOutTarget isecEnlTarget isecDisTarget isecPofileShow isecConfirm isecDecom isecIkeShowPAll isecIpsecShowIf	VxWorks IPSec management commands
disInsecureShells enlInsecureShells statInsecureShells disSecureShells enlSecureShells statSecureShell	Vxworks specific
sshKeyClear sshKeyGenerate sshKeyShow	Vxworks specific
mdp	Deplist support
firmwareVersionShow swDownload itgChanStateShow disiVGW enaVGW vgwShowAll vgwShow	Media Card specific

Commands	Description
adminUserPasswordChange adminUserCreate adminUserDelete adminAccountShow	Vxworks specific
unpackEmHelp unpackVTHelp	Vxworks specific
rdopen rdgo rd rds rdshow rdall rdtail rdhead rdnext rdprev rdsconvert	RPT report management commands.
lkup	Vxworks specific
devs	Vxworks specific
moduleShow	Vxworks specific
arpPrivLogDisable arpPrivLogEnable	Vxworks specific

Chapter 38: UDT Universal Digital Trunk card Command Line Interface

This chapter describes the UDT Universal Digital Trunk card command line interface (CLI).

- Command Line Interface on page 665
- Main menu on page 666
- System Maintenance on page 667
- UDT Administration on page 672
- UDT Maintenance on page 674
- Remote access to the UDT card on page 677

Command Line Interface

The UDT card has two Command Line Interface (CLI) levels:

- basic level
- advanced level (in debug mode) which includes all the commands available at the basic level, as well as, additional commands for debug purposes only.

CLI commands are organized in a tree structure similar to file system folders and files. See Figure 8: CLI command tree structure on page 666.

To navigate the CLI tree use the following commands (similar to the Unix operating system):

- ls - lists commands and directories in current directory,
- cd<name> - moves to the specified directory,
- cd .. - returns one level up
- ? – for help (displays a short description of each command or directory in the current level).

Characters input are case sensitive.

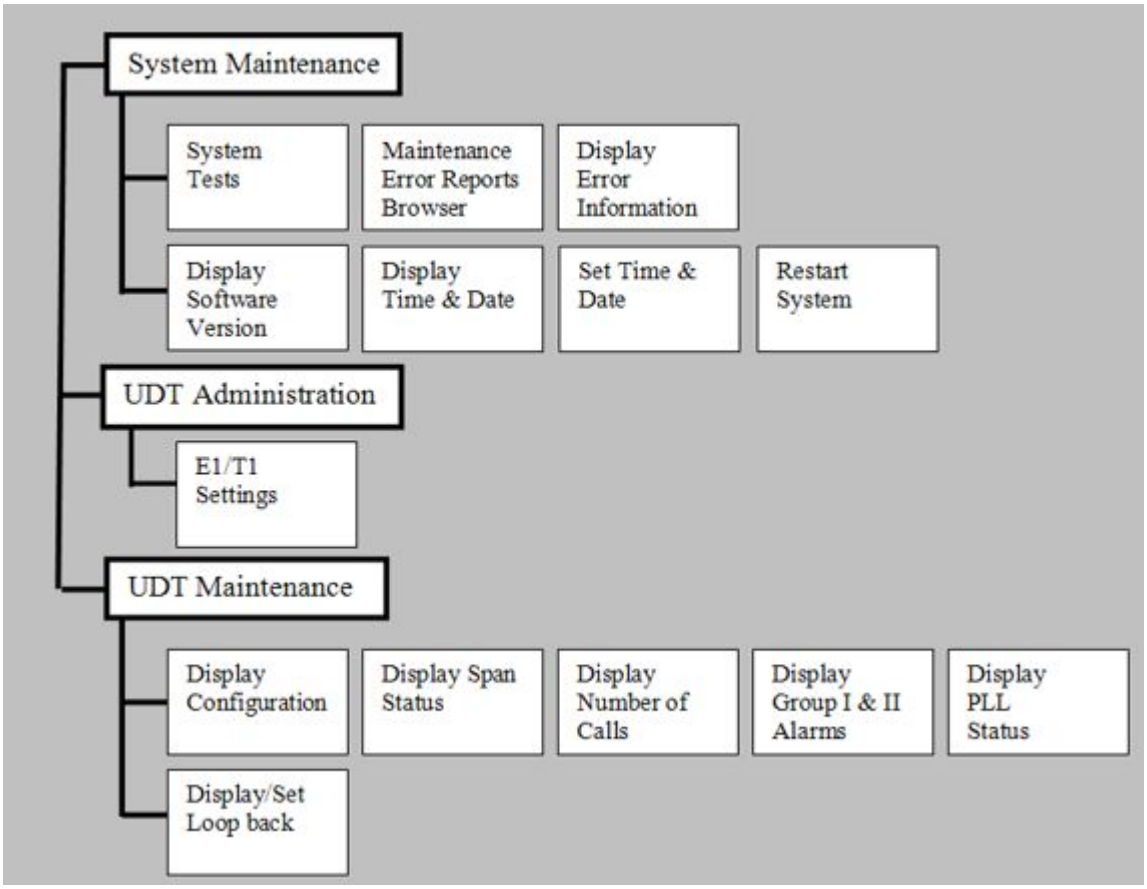


Figure 8: CLI command tree structure

Main menu

The following management activities groups are available: smaint - System Maintenance directory; udtadmin - UDT Administration; udtmaint - UDT Maintenance directory.

This is the top layer, which is used for navigation purposes only.

Available commands:

- ls - lists commands and directories in current directory,
- cd<name> - moves to the specified directory,
- ? – for help (displays a short description of each command or directory in the current level).

ls command

In response to the ls command, the following is displayed:

```
UDT [1/] ls

smaint/     udtadmin/     udtmaint/     ?
```

? command

In response to the ? command, the following is displayed:

```
UDT [2/] ?

smaint              System Maintenance directory
udtadmin            Span Administration directory
udtmaint            Span Maintenance directory
```

System Maintenance

The following commands are available within the System Maintenance directory

- ls - lists commands and directories in current directory,
- cd<name> - moves to the specified directory,
- cd .. - moves to root directory
- ? – for help (displays a short description of each command or directory in the current level).
- stest - System Test directory
- crestart - Card restart
- mreport - Maintenance Error Reports
- qver - Display software version
- showerr - Display Error Information
- stad - Set time and date
- ttad - Display time and date

ls command

In response to the ls command, the following is displayed:

```
UDT [19 /] cd smaint
UDT [20 /smaint] ls
stest/     ?        crestart   mreport    qver       showerr
stad       ttad
```

? command

In response to the ? command, the following is displayed:

```
UDT [21 /] cd smaint
UDT [22 /smaint] ?
stest        System Test directory.
crestart     Restart System.
mreport      Browse Maintenance Error Report
             in order to analyze system problems.
qver         Display current software version.
shower       Display information for specific error code.
stad         Set current time and date.
ttad         Display current time and date.
```

System Test

The following commands are available within the System Test directory

- ls - lists commands and directories in current directory,
- cd<name> - moves to the specified directory,
- cd .. - moves to root directory
- ? – for help (displays a short description of each command or directory in the current level).
- inserv - for in-service system test
- outserv - for out-of-service system test

Objective: perform system component tests.

In response to ls command, the following is displayed:

```
UDT [23 /] cd smaint
UDT [24 / smaint] cd stest
UDT [25 /smaint/stest] ls
?          inserv    outserv
```

In response to ? command, the following is displayed:

```
UDT [25 /] cd smaint
UDT [26 / smaint] cd stest
UDT [27 /smaint/stest] ?
inserv     Perform in-service system test.
outserv    Perform out-of-service system test.
```

In response to inserv command, the following is displayed:

```
UDT [28 /] cd smaint
UDT [29 / smaint] cd stest
UDT [30 /smaint/stest] inserv
Performing in service test ... Test passed.
```

In response to outserv command, the following is displayed:

```
UDT [31 /] cd smaint
UDT [32 / smaint] cd stest
UDT [34 /smaint/stest] outserv
Perform service impacting test? (Yes, (No))y
```

crestart command

Objective: manual reset of the card.

In response to the crestart command, the following is displayed:

```
UDT [35 /] cd smaint
UDT [36 /smaint] crestart
Restart the card? (Yes, (No))y
```

mreport command

Objective: browse Maintenance Error Reports in order to analyze system problems.

All reports are time stamped (according to the time & date set by using the stad command) and contain verbal information regarding the nature of the problem. To exit before maintenance report file has been presented in full, use *<CR> (star) during printout.

The maintenance reports have the following format: <serial number>: <severity> < error code> <timestamp> <error text>

For example:

```
UDT [37 /] cd smaint
UDT [38 /smaint] mreport
00024 INFO INIT041 06-05 06:30:48:204 POWER-UP RESET
00025 INFO PRI195 06-05 06:33:50:480 Hardware Self test succeeded
```

showerr command

In addition to the error text in the message itself, the UDT card provides on-line help for error messages. The CLI command receives as input the unique error code and prints the related information for this message: <syntax> - definition of the message syntax. Meaning: what does this message indicate. Parameters: description of the message parameters (fields). Action: steps the administrator can follow to isolate the problem and/or fix it. Impact: possible visual/ physical/higher level effects of the event.

For example:

```
UDT [39 /] cd smaint
UDT [40 /smaint] showerr  PRI025
     UDT [3 /smaint] showerr PRI025
     PRI025:         E1  alarm  <alarm_name>  <alarm_state>  on  span
     <span_number>
     Meaning:    E1 Alarm Group II condition.
     Parameters: <alarm_name> -  RAI (remote alarm indication)
                                 LOS (loss of signal)
                                 AIS (alarm indication signal)
                                 LFAS  (loss  of  frame  alignment
     signal)
                                 CLMAS    (loss    of    multi-frame
     alignment signal)
                 <alarm_state> - occurred
                                 persisted
                                 cleared
                 <span_number> - span 1.
     Action:     State "persisted" or "occurred" - Check the cabling
     and far-end
                 equipment.
                 State 'cleared' - None.
     Impact:    State "persisted" or 'occurred' - The specified span
     is not able
                 to carry calls.
                 State "cleared" - If there was no other alarms, then
     that span is
            now able to carry calls.
```

qver command

Objective: display software version.

For example:

```
UDT [41 /] cd smaint
UDT [42 /smaint] qver
Boot version:           1.11
Main Load version:      1.0.1
FPGA version:           00af
```

ttad command

Objective: display time and date on the UDT card.

For example:

```
UDT [45 /] cd smaint
UDT [46 /smaint] ttad
Card time: Feb. 10, 2008 23:45:06
```

stad command

Objective: set time and date on the UDT card.

For example:

```
UDT [47 /] cd smaint
UDT [48 /smaint] stad <month> <day> <year> <hour> <minutes> <seconds>
 Stad 2 20 2008 0 0 0
 Card time set to: Feb. 20, 2008 10:30:28
```

UDT Administration

The following commands are available within the UDT Administration directory

- ls - lists commands and directories in current directory,
- cd<name> - moves to the specified directory,
- cd .. - moves to root directory

- ? – for help (displays a short description of each command or directory in the current level).
- E1T1Settings – set/modify the E1/T1 settings. The card is restarted after saving the changes.

ls command

In response to the ls command, the following is displayed:

```
UDT [57 /] cd udtmaint
UDT [58 /udtmaint] ls
?       AlarmStatus   ChannelStatus   Lpbck       PllStatus
        SpanStatus    UdtConfig
```

? command

In response to the ? command, the following is displayed:

```
UDT [51 /] cd udtadmin
UDT [52 / udtadmin] ?
```

E1T1Settings Display/Modify E1/T1 Settings
The card is restarted after saving the changes

E1T1Settings command

Objective: set/modify the E1/T1 parameters.

For Protocol type E1, set the following parameters:

- Usage - select one of the following values: BCH, DTI2, PRI2, DDCS
- CRC4 - select one of the following values: NO, YES
- AIS in TS16 – select one of the following values: (NO), YES

  available only for DTI2 Usage

For example:

```
UDT [3 /] cd udtadmin
UDT [4 /udtadmin] E1T1Settings
E1/T1 Settings:
Protocol: E1
Usage:PRI2
CRC4: No
Modify, Save, Cancel: m
Protocol E1
Usage (PRI2, 1-BCH, 2-DTI2, 4-DDCS ):2
CRC4 (No, 1-Yes ): <CR>
Ais in ts16 (No, 1-Yes ): <CR>

New E1/T1 Settings:
Protocol: E1
Usage:DTI2
CRC4: No
Ais in ts16: No

Modify, Save, cancel: s
```

UDT Maintenance

The following commands are available within the UDT Maintenance directory

- ls - lists commands and directories in current directory,
- cd<name> - moves to the specified directory,
- cd .. - moves to root directory
- ? – for help (displays a short description of each command or directory in the current level).
- AlarmStatus - display group 1 and 2 alarms;
- ChannelStatus - display the number of channels which have active digital padding;
- Lpbck - display/Set loopback;
- PllStatus – display PLL status;.
- SpanStatus - display span status;
- UdtConfig – display span configuration.

ls command

In response to the ls command, the following is displayed:

```
UDT [57 /] cd udtmaint
UDT [58 /udtmaint] ls
?       AlarmStatus   ChannelStatus   Lpbck       PllStatus
        SpanStatus    UdtConfig
```

? command

In response to the ? command, the following is displayed:

```
UDT [59 /] cd udtmaint
UDT [60 / udtmaint] ?

UdtConfig     Display UDT configuration (protocol, line coding,
              Yellow alarm mode, framing, connection,
              Clock reference definitions)
SpanStatus    Display span status (Disable/Enable)
ChannelStatus Display number of calls and details about active
              calls
AlarmStatus   Display group 1 and 2 alarms
PllStatus     Display PLL status
Lpbck         Set/Clear/Display remote/local loopback for PRI/DTI span
```

Alarm Status command

Objective: display group 1 and 2 alarms.

For example:

```
UDT [67 /] cd udtmaint
UDT [68 /udtmaint] AlarmStatus
Group I alarms  : NONE
Group II alarms : LOS
```

ChannelStatus command

Objective: display the number of channels which have active digital padding.

For example:

```
UDT [65 /] cd udtmaint
UDT [66 /udtmaint] ChannelStatus
Busy channels: 1 4 7 10 13 16 19 22
Total: 8
```

Lpbck command

Objective: Set/Clear/Display remote/local loop-back for span.

For example:

```
UDT [71 /] cd udtmaint
UDT [72 /udtmaint] Lpbck
Current settings:
No loopbacks per loop

Local loopback per channel(s): No loopbacks
Remote loopback per channel(s): No loopbacks

UDT [73  /udtmaint] Lpbck ?
Set/Clear/Display loopback for PRI/DTI span.
To Set/Clear loopback:
Syntax: Lpbck <Loop Mode><On_Off> [<chan> - optional]
Where:Loop Mode: 0 = Remote(line loopback), 1 = Local
On_Off: 0 = Clear, 1 = Set
For E1 span:chan: 1..15, 17..31
For T1 span:chan: 1..23
To Display loopback:
Syntax: Lpbck
```

PLLStatus command

Objective: display PLL status.

For example:

```
UDT [69 /] cd udtmaint
UDT [70 /udtmaint] PllStatus
 Clock Controller: Disabled
 PLL mode: FREE RUN Sync src: FREERUN
 previous: ACQUISITION           FREERUN
```

SpanStatus command

Objective: display span status. Is it enabled or disabled

For example:

```
UDT [63 /] cd udtmaint
UDT [64 /udtmaint] SpanStatus
mode: DTI
status:  Enabled
```

UdtConfig command

Objective: display span configuration.

The following information is printed: protocol, usage, line coding, yellow alarm mode, framing, LBO and clock reference definitions.

For example:

```
UDT [8 /] cd udtmaint
UDT [9 /udtmaint] UdtConfig

UDT configuration:

Universal Clock Controller: Equipped
Clock Reference Sync. Source: Primary

Protocol: E1
Usage: PRI2
Connection: RJ48 120 ohm
Framing: AFM
```

Remote access to the UDT card

The UDT card can be remotely accessed only with a modem. A modem can be connected to the UDT card serial port 9-pin connector.

The RS-232 setup is as follows:

- Speed: 9600
- Data bits: 8
- Parity: N
- Stop bit: 1

Chapter 39: Linux base CLI commands

This chapter lists Linux base CLI commands. Type **(linuxbase-command) -h | --help** at the command prompt to display a brief summary of the CLI command, as shown in Table 108: CLI command help on page 679. Type **man (linuxbase-command)** at the command prompt for a more detailed description, as shown in Table 109: man command example on page 679.

Table 108: CLI command help

```
$ poos --help
Usage:
poos (patch_id)|-app *(app_name)*|--help,-h

Options:
(patch_id)
Deactivate patch with (patch_id) handle.

-app *(app_name)*
Deactivate all patches for the application (app_name).

--help
Print this help message and exit.
```

Table 109: man command example

```
$ man poos
```

```
POOS(1) User Contributed Documentation POOS(1)

NAME
poos - Put a patch out of service.

SYNOPSIS
poos (patch_id)| -app (app_name) | --help,-h

DESCRIPTION
Remove a patch from service. The patch is removed from service from all processes in which it was in service.

OPTIONS
(patch_id)
Deactivate patch with (patch_id) handle.

-app (app_name)
Deactivate all patches for the application (app_name).

--help Print this help message and exit.

EXAMPLES
```

```
Deactivate patch with 2 handle
$ poos 2
Patch handle: 2
Please ensure that the application solid is stopped before proceeding patch un-installation.
Do you want to continue patch un-installation? (Y/N) [N]? y
Performing the uninstallation:
Performing uninstall RPM patch...
Preparing... ########################################### [100%]
1:cs1000-solid ########################################### [100%]
executing Solid DB post install...
Installation Avaya Solid database server completed.
Unstalling the Solid database server package done

Done.
The RPM patch uninstallation is completed.
The patch 2 has been deactivated successfully.

Deactivate all sunAm patches
$ poos -app sunAm
Patch handle: 0
Performing the uninstallation:
The patch 0 has been deactivated successfully.

SEE ALSO pload, pout, pins, pstat, plis

5.50 2007-12-18 POOS(1)
```

Table 110: Common CLI commands

Command	Description
appVersionShow	Print the server's application software version.
baseVersionShow	Print the server's base software version.
echo	Display a line of text on the terminal screen.
find	Search for files in a directory hierarchy.
ftp	Transfer files to and from a remote network site.
ifconfig	Configure a network interface.
ls	List directory contents
man	Format and display the online manual pages.
printenv	Print all or part of environment.
scp	Copy files between hosts on a network using ssh.
sftp	Transfer files to and from a remote network site secure file transfer program.
ssh	Run OpenSSH SSH client (remote login program) to provide secure encrypted communications

Command	Description
	between two untrusted hosts over an insecure network.
su	Run a shell with substitute user and group IDs
swVersionShow	Print the server's software version.
telnet	Communicate with another host using the TELNET protocol.
whoami	Print the user name associated with the current effective user ID.

Table 111: systemadmin CLI commands

Command	Description
appinstall	Install applications. **Note:** Do not use the appinstall command unless you are directed to use it by Avaya support.
appstart	Stop, start, or restart applications.
appstart dbcom start	Start the DB engine.
appstart dbcom stop	Stop the DB engine.
appstart dbcom status	Check the status of the DB engine.
appstart dbcom restart	Restart the DB engine.
baseparamsconfig	Configure base parameters.
datetimeconfig	Configure the date and time.
dnsconfig	Configure DNS values.
ecnconfig	Configure Explicit Congestion Notification settings.
hostconfig	Configure the static lookup table for host names.
networkconfig	Configure network settings.
ntpconfig	Configure Network Time Protocol settings.
reboot	Reboot the entire system.
routeconfig	Configure routing entries.
syslogFacilitySet	Set the facility value.
syslogLevelSet	Set a value for level.
syslogShow	Display syslog processes.

Command	Description
sysrestore	Perform a restore of the application data (backed up by sysbackup).
timeadj	Specify system clock parameters.
upgrade	Select the backup data source and reinstall Linux base.

Note:

You might need to add the primary host entry in the backup and member server before you can access them using the **hostconfig** command.

The command syntax is **admin2 ---> hostconfig add -ip <PRIMARY SERVER IP> -host <PRIMARY SERVER HOST NAME> -domain <PRIMARY SERVER DOMAIN NAME>**.

Table 112: maintadmin CLI commands

Command	Description
gnome-system-monitor	
wireshark	
pcap	
gryphon	

Table 113: logadmin CLI commands

Command	Description
Authors note: commands not listed at this time	

Table 114: securityadmin CLI commands

Command	Description
basefirewallconfig	Configure firewall settings.
checkIPsecStatus	
disableAllTargets	Disable all IPSec targets and remove all IPSec data.
harden	Manage CS 1000 hardening items.
sshconfig	Configure SSH keys
masterfirewallconfig	
nfsexportsconfig	
sshconfig	Tool to regenerate and distribute SSH host key on aMember UCM server .

Table 115: backupadmin CLI commands

Command	Description
sysbackup	Perform a system backup (both base and applications).

Table 116: patchadmin CLI commands

Command	Description
pins	Put the patch in service.
plis	Show detailed information about the patch.
pload	Load the patch into the system database.
poos	Put the patch out of service.
pout	Unload the patch from the system database.
pstat	Show a list of installed patches.

Table 117: dbadmin CLI commands

Command	Description
Author's note: No commands listed at this time	

Table 118: timeadmin CLI commands

Command	Description
datetimeconfig	Configure the date and time.
ntpconfig	Configure Network Time Protocol settings.
timeadj	Allow tuning of system clock frequency in case the clock gained or lost time.

Table 119: harden CLI commands

Command	Description
harden audit status	Displays the status of the Linux Audit Daemon.
harden banners set/file	Modify the banner text. The banner text will be replaced by the content from the file.
harden banners status	Enables or disables the pre-login banners.
harden basic	Apply basic hardening changes. Ensures that the basic hardening items are in secure status.
harden basic reapply	Apply basic hardening changes. Ensures that the basic hardening items are in secure status.

Command	Description
harden coredumps status	Enables or disables the coredump service.
harden ftp status	Shows that FTP service is turned on or off.
harden help	Displays help information for using the command.
harden nettools status	Enables or /disables the nettools service.
harden nfs help	Displays help information for using the command.
harden nfs on	Enables Network File System (NFS) when deploying the primary security server.
harden nfs off	Disables NFS after deployment is complete.
harden nfs status	Shows that NFS is turned on or off.
harden passwd_days off	Disable previously configured parameters.
harden passwd_days on	Enables previously configured parameters.
harden passwd_days set -max	Set value the value of the PASS_MAX_DAYS parameter. The default value is 90.
harden passwd_days set -min	Set the value of the PASS_MIN_DAYS parameter. **Note:** This parameter must be set to a value >or = 1. The default value is 1.
harden passwd_days status	Provides the current value of the parameters from hardening storage.
harden rlogin	Apply hardening to remote logins.
harden rlogin status	Shows if hardening for remote logins is on or off.
harden ssh_filter -allow add –subnet	Add a subnet to the allowed list.
harden ssh_filter -allow del	Delete a host IP 1 from the allowed list.
harden ssh_filter -allow del -IP	Delete a host IP from the corresponding (allow or deny) filtration list.
harden ssh_filter -allow del –subnet	Delete a subnet from the allowed list.
harden ssh_filter -deny add -IP	Add a host to the deny list.
harden ssh_filter -deny del -IP	Delete a host IP from the deny list.
harden ssh_filter -deny del <number>	Delete a host IP from the corresponding filtration list. Each host entity (per line) has logical ordinal number in XML file storage. <number> is this sequence number.

Command	Description
harden ssh_filter status	Shows the list of the names of the hosts which are allowed to connect to Linux Base by SSH.
harden status	Retrieve the status of Linux Base Enhanced Hardening options.
harden telnet status	Shows that telnet service is turned on or off.
harden tftp status	Shows that TFTP service is turned on or off.

Table 120: VxWorks CLI commands

Command	Description
isssDecom	Clean up ISSS settings and delete ISSS configuration files.
isssReset	Reset ISSS configuration.
isssShow	Print out ISSS settings.

Index

C

CDSP,30 59
CMAJ,30 59
CMIN ALL,30 137
CPED,30 59

D

DISL,30 59

E

END,30 59
ENLL,30 59

L

LDIS,30 59
LENL,30 59
LOOP,30 59

R

RPED,30 59

S

SHLF,30 59
SLFT,30 59
STAT,30 59
STEI,30 59
Succession 1000 system 183

T

TEIT,30 59
TEST,30 59
TTSM,30 59
TTWI,30 59

U

UNTT,30 59