Nways Multiprotocol Switched Services Server

Interface Configuration and Software User's Guide

SC30-3818-04

Nways Multiprotocol Switched Services Server

Interface Configuration and Software User's Guide

SC30-3818-04

Note

Before using this document, read the general information under “Notices” on page xxi.

Fifth Edition (February 1999)

This edition applies to Version 2.2 of the IBM Multiprotocol Switched Services (MSS) and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address below.

IBM welcomes your comments. A form for readers' comments is provided at the back of this publication. If the form has been removed, you may address your comments to:

International Business Machines Corporation

Design and Information Development

Department CGF

P.O. Box 12195

Research Triangle Park, NC 27709-9990

U.S.A.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 1996, 1998. All rights reserved.
Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

Figures xvii

Tables xix

Notices xxi

Notice to Users of Online Versions of This Book xxiii

Trademarks xxv

Preface xxvii
Conventions Used in This Manual xxvii
MSS Server Library xxviii
Summary of Changes For Version 2.2 xxviii
Editorial Changes xxix

Part 1. User's Guide 1

Chapter 1. Getting Started 3
Before You Begin 3
Migrating to the Current Release 3
Accessing the Software Using Local and Remote Consoles 3
Local Consoles 4
Remote Consoles 5
Logging In Remotely or Locally 5
Reloading the Router 6
Exiting the Router 6
Discussing the User Interface System 6
Understanding the First-Level User Interface 6

Chapter 2. Using the Software 9
Entering Commands 9
Connecting to a Process 9
Identifying Prompts 10
Getting Help 10
Exiting a Lower Level Environment 11
Getting Back to OPCON 11
Some Configuration Suggestions 11
Creating a First Configuration 11
Basing a Configuration on an Existing Configuration 12
Accessing the Second-Level Processes 14
Accessing the Configuration Process, CONFIG (Talk 6) 14
Accessing the Console Operating/Monitoring Process, GWCON (Talk 5) . . 15
Accessing the Secondary ELS Console Process, ELSCon (Talk 7) 15
Accessing the Third-Level Processes 16
Accessing Network Interface Configuration and Operating Processes . . . 16
Accessing Feature Configuration and Operating Processes 17
Accessing Protocol Configuration and Operating Processes 18
Command Completion 20
Online Help When Command Completion is Enabled 20
Online Help When Command Completion is Disabled 22
Command History 22
Repeating a Command in the Command History 23

© Copyright IBM Corp. 1996, 1998

Repeating a Series of Commands in the Command History 23

Chapter 3. Using MSS Server Firmware 27
Accessing the Firmware Prompt 27
Boot Options Available for the MSS Server 27
Attended Mode 28
Unattended Mode 28
Starting the MSS Server Firmware 28
The Function Keys 29
Obtaining Help 29
Managing the Configuration 29
Selecting the Boot Sequence 30
Selecting a Device To Test 30
Using the Utilities 32
Setting the Supervisory Password 33
Enabling Unattended Start Mode 34
Disabling Unattended Start Mode 35
Removing Supervisory Password 36
Updating System Firmware 37
Displaying the Event/Error Log 37
Viewing Vital Product Data 40
Copying Remote Files 41
Setting Up Remote Initial Program Load 42
Manipulating the Dead Man Timer 43
Change Management 43

Chapter 4. Getting Started with Configuring the 8210 47
Physical Access Methods 47
SLIP Addresses 48
Serial Port and Data/Fax Modem Default Settings 49
Configuration and Monitoring Tools 49
Fax Accumulation 51
Local and Remote Console Access 51
Remote Voice Access 51
File Transfer 52
Initial Configuration 52
First Example 52
Second Example 52
Tips for Managing Configuration Problems 53
Reconfiguring 53
Quick Configuration 53
Completing the Configuration After Quick Configuration 53
How Software Files Are Managed 54
How to View the Files 54
How to Reset the IBM 8210 54
File Transfer Using TFTP 55
Storing Configuration Files Using the Command Line Interface or the Web Browser Interface 55
Changing the Statuses of Files 55
Using the Configuration Program to Manage the Configuration Files 55
Using the Set Commands 56
Other Change Management Functions 56
Using the Copy Command 57
Using the Lock Command 57
Using the Unlock Command 57

Chapter 5. Using the World Wide Web Interface 59
Connecting to the World Wide Web Interface 59
Rules for Using the Web Interface 59
Home Page Structure 60
Configuration and Console Menu 61
Event Logging System 62
Operator Console 62
Device Configuration 62
History Function 63
Help System for the Web Browser Interface 63
Quick Configuration Using the Web Browser Interface 63
Guided Configuration 63
Devices 64
LAN Emulation 64
Bridging 65
IP 65
IPX 66
An Example of Quick Configuration Using the Web Browser Interface . . . 66

Chapter 6. MSS Server Voice/Data/Fax Modem Support 67
Installation of the Voice/Data/Fax Modem 67
Data/Fax Modem 67
MSS Server Voice Access Using the Voice/Data/Fax Modem 67
Performance Information 68
Remote Service 68
Network Monitoring 68
Configuration 68
MSS Server Voice Pager Support 69
Voice Pager Configuration Parameters 69
Voice Pager Messages 70
Maintenance Log 70
Maintenance Log Configuration Parameter 70
Voice/Data/Fax Modem Menu Items 70
Option 1—Reset 71
Option 2—Status and Statistics 71
Option 3—Reports 72
Option 4—Event Logs 73
Option 5—Configuration 73
Option 6—Device Presence and Status Report 73
Option 7—Resend Last Fax Report 74
Option 8—Disconnect Call 74
Option 9—Repeat Menu 74

Chapter 7. The OPCON Process and Commands 75
What is the OPCON Process? 75
Accessing the OPCON Process 75
OPCON Commands 75
Configuration 76
Console 76
Diags 77
Divert 77
Els 78
Event 78
Flush 78
Halt 78
Intercept 79

Logout 79
Memory 79
Ping 80
Reload 81
Status 81
Talk 82
Telnet 83

Chapter 8. The CONFIG Process (CONFIG - Talk 6) and Commands . . . 85
What is CONFIG? 85
Config-Only Mode 86
Quick Configuration 86
Configuring User Access 87
Configuring Spare Interfaces 88
Resetting Interfaces 90
Using System Dumps 91
Entering and Exiting CONFIG 92
CONFIG Commands 92
Add 93
Boot 94
Change 95
Clear 96
Delete 97
Disable 98
Enable 99
Event 101
Feature 101
List 102
Load 103
Network 103
Patch 104
Performance 105
Protocol 105
Qconfig 106
Set 106
System Retrieve 110
System View 111
Time 111
Unpatch 112
Update 112
Write 112

Chapter 9. Using BOOT Config to Perform Change Management 113
Understanding Change Management 113
Using the Trivial File Transfer Protocol (TFTP) 113
Loading an Image at a Specific Time 114

Chapter 10. Configuring Change Management 115
Accessing the Change Management Configuration Environment 115
Change Management Configuration Commands 115
Add 116
Copy 116
Describe 118
Disable 118
Enable 118
Erase 119

List 121
Lock 121
Set 122
TFTP 123
Timedload 125
Unlock 127

Chapter 11. The Operating/Monitoring Process (GWCON - Talk 5) and Commands 129
What is GWCON? 129
Entering and Exiting GWCON 129
GWCON Commands 130
Activate 130
Buffer 130
Clear 131
Configuration 132
Disable 134
Error 134
Event 135
Feature 135
Interface 135
Memory 136
Network 137
Performance 138
Protocol 138
Queue. 139
Reset 140
Statistics 140
Test 140
Uptime 141

Chapter 12. The Messaging (MONITR - Talk 2) Process 143
What is Messaging (MONITR)? 143
Commands Affecting Messaging 143
Entering and Exiting the Messaging (MONITR) Process 143
Receiving Messages 143

Chapter 13. Using the Event Logging System (ELS) 145
What is ELS? 145
Entering and Exiting the ELS Configuration Environment 146
Event Logging Concepts 146
Causes of Events 146
Interpreting a Message 147
Using ELS 149
Managing ELS Message Rotation 150
Capturing ELS Output Using a Telnet Connection on a UNIX Host 150
Configuring ELS So Event Messages Are Sent In SNMP Traps 151
Using ELS to Troubleshoot a Problem 151
ELS Example 1 151
ELS Example 2 152
ELS Example 3 152
Using and Configuring ELS Remote Logging 153
Syslog Facility and Level 153
Remote Workstation Configuration 153
Configuring the 8210 for Remote Logging. 155
Remote Logging Output 157

Additional Considerations . . . 160
Using ELS Message Buffering . . . 161

Chapter 14. Configuring and Monitoring the Event Logging System (ELS) . 165
Accessing the ELS Configuration Environment . . . 165
ELS Configuration Commands . . . 165
Add . . . 166
Advanced . . . 166
Clear . . . 166
Default . . . 167
Delete . . . 167
Display . . . 167
List . . . 168
Nodisplay . . . 169
Noremote . . . 170
Notrace . . . 171
Notrap . . . 172
Remote . . . 173
Set . . . 174
Trace . . . 179
Trap . . . 179
ELS Message Buffering Configuration Commands . . . 180
Entering and Exiting the ELS Operating Environment . . . 184
ELS Monitoring Commands . . . 184
Advanced . . . 185
Clear . . . 185
Display . . . 185
Files Trace TFTP . . . 186
List . . . 186
Nodisplay . . . 189
Noremote . . . 189
Notrace . . . 190
Notrap . . . 191
Packet Trace . . . 192
Remote . . . 192
Remove . . . 194
Restore . . . 194
Retrieve . . . 194
Save . . . 194
Set . . . 194
Statistics . . . 200
Trace . . . 202
Trap . . . 202
View . . . 203
Packet-trace Monitoring Commands . . . 204
ELS Message Buffering Monitoring Commands . . . 207

Chapter 15. Configuring and Monitoring Performance . . . 213
Performance Overview . . . 213
Performance Reporting Accuracy . . . 213
Accessing the Performance Configuration Environment . . . 213
Performance Configuration Commands . . . 214
Disable . . . 214
Enable . . . 214
List . . . 214
Set . . . 215

Accessing the Performance Monitoring Environment . . . 215
Performance Monitoring Commands . . . 215
Disable . . . 216
Enable . . . 216
List . . . 216
Report . . . 216
Set . . . 216

Chapter 16. Using FDDI . . . 219
Fiber Distributed Data Interface (FDDI) Overview . . . 219
Token-Passing Ring Network . . . 219
Primary and Secondary Rings . . . 219
Attachment of Devices . . . 219
Differences Between FDDI and Token-Ring . . . 220
Device Classes A and B . . . 220
FDDI Network Diagram . . . 221

Chapter 17. Configuring and Monitoring FDDI . . . 223
Accessing the FDDI Configuration Commands . . . 223
FDDI Configuration Commands . . . 223
List . . . 223
Set . . . 224
Accessing FDDI Monitoring Commands . . . 225
FDDI Monitoring Commands . . . 226
List . . . 226
Srt-stats . . . 226
FDDI Interfaces and the GWCON Command . . . 226
Statistics Displayed from FDDI Interfaces . . . 227

Part 2. ATM and LAN Emulation . . . 231

Chapter 18. Overview of LAN Emulation . . . 233
LAN Emulation Benefits . . . 233
LAN Emulation Components . . . 234
Addressing in ATM . . . 235
ESI . . . 236
ATM Addresses of LAN Emulation Components . . . 236
Overview of Related ILMI Functions . . . 237
Manual Configuration of the Signaling Version . . . 237
Locating the LECS Using ILMI . . . 237
Overview of the LECS Function . . . 238
Sample Situations for Use of the LECS Assignment Policies . . . 240
More Information About TLVs . . . 241
Connecting to the LES . . . 242
Address Registration . . . 243
Address Resolution . . . 243
Connecting to the BUS . . . 243
BUS Functions . . . 244
BUS Data Packet Filtering . . . 245
Establishing Data Direct VCCs . . . 245
Overview of Extensions for LAN Emulation . . . 246
Broadcast Manager . . . 246
BCM Support for IP . . . 247
BCM Support for IPX . . . 247
BCM Support for NetBIOS . . . 248
BCM Support for Source Route Bridging . . . 248

LAN Emulation Reliability 248
LAN Emulation Security 250
BUS Monitor 251
BUS Police 252
LECS Database Synchronization 252
SuperELAN 252
SuperELAN II 253
Key Configuration Parameters for LAN Emulation 254

Chapter 19. Using ATM 255
ATM and LAN Emulation 255
How to Enter Addresses 255
ATM-LLC Multiplexing 256
ATM SuperELAN II Configuration Concepts 256
Configuring a SuperELAN II 256
SuperELAN II Spanning Tree 257
Redundant SuperELANs 258
Token Ring SuperELANs 259
Configuring Routing Protocols on SuperELAN II Interfaces 260
Migration to SuperELAN II 260
Sample SuperELAN II Configuration 260
ATM Virtual Interface Concepts 265
Advantages of Using ATM Virtual Interfaces 265
Disadvantages of using ATM Virtual Interfaces 266

Chapter 20. Configuring and Monitoring ATM 267
Accessing the ATM Interface Configuration Process 267
ATM Configuration Commands 268
ATM Interface Configuration Commands 269
Add 269
List 269
QoS Configuration 270
Remove 270
Set 270
Enable 274
Disable 274
Accessing the Virtual ATM Interface Configuration Process 275
ATM Virtual Interface Configuration Commands 275
Add 275
List 275
Remove 276
Accessing the ATM Monitoring Process 276
ATM Monitoring Commands 277
Interface 277
LE-Services 277
ATM-LLC 277
ATM Interface Monitoring Commands (ATM INTERFACE+ Prompt) 278
List 278
Trace 279
Wrap 280
ATM-LLC Monitoring Commands 281
List 281
ATM Virtual Interface Monitoring Commands 281

Chapter 21. SuperELAN Services 283
Accessing the SuperELAN II Configuration Process 283

SuperELAN II Configuration Commands . . . 283
Add . . . 283
Delete . . . 284
List . . . 284
Migrate . . . 285
Rename . . . 287
Work with SuperELAN . . . 287
Selected SuperELAN Configuration . . . 287
Add ELAN to SuperELAN . . . 288
Broadcast-Manager . . . 288
Delete ELAN from SuperELAN . . . 288
Disable . . . 289
ELANs . . . 289
Enable . . . 289
List . . . 290
Set . . . 290
Trace . . . 292
Work with ELAN . . . 293
VLANs . . . 294
Selected ELAN Configuration . . . 294
Disable . . . 294
Enable . . . 295
LE-Client Configuration . . . 295
LES-BUS Configuration . . . 295
List . . . 295
Spanning Tree Port Parameters . . . 296
Trace . . . 296
Accessing SE-Services Monitoring Process . . . 297
SE Services Monitoring Commands . . . 297
Create . . . 297
List . . . 298
Work with SuperELAN . . . 298
Selected SuperELAN Monitoring Commands . . . 298
Broadcast Manager . . . 299
Clear . . . 299
Create . . . 299
Disable . . . 299
Display . . . 300
Enable . . . 300
ELANs . . . 300
Flush . . . 301
List . . . 301
Restart . . . 302
Set Cache . . . 302
Show . . . 303
Trace . . . 303
Work with ELAN . . . 304
VLANs . . . 304
Selected ELAN Monitoring Commands . . . 305
Disable . . . 305
Display . . . 306
Enable . . . 306
Flush . . . 306
LEC . . . 307
LES-BUS . . . 307
List . . . 307

Restart . . . 308
Show . . . 308
Trace . . . 308

Chapter 22. Using LAN Emulation Clients . . . 311
LAN Emulation Client Overview . . . 311

Chapter 23. Configuring and Monitoring LAN Emulation Clients . . . 313
Configuring LAN Emulation Clients . . . 313
Add . . . 313
Config . . . 314
List . . . 314
Remove . . . 315
Configuring an ATM Forum-Compliant LE Client . . . 315
ARP Configuration . . . 316
Frame . . . 318
IP-Encapsulation (for Ethernet ATM Forum-Compliant LEC only) . . . 318
List . . . 319
LLC . . . 319
QoS . . . 319
RIF-Timer (for Token-Ring Forum-compliant LEC only) . . . 319
Set . . . 319
Source-Routing (for Token-Ring Forum-Compliant LEC only) . . . 329
Configuring an IBM LE Client . . . 330
Frame . . . 330
IP-Encapsulation (for Ethernet-IBM LEC only) . . . 331
List . . . 331
LLC . . . 331
RIF-Timer (for Token-Ring-IBM LEC only) . . . 332
Set . . . 332
Source-routing (for Token-Ring-IBM LEC only) . . . 335
LLC Configuration Commands . . . 336
List . . . 336
Set . . . 336
Accessing the LEC Monitoring Environment . . . 337
LEC Monitoring Commands . . . 338
List . . . 339
LLC . . . 342
MIB . . . 342
QoS Information . . . 346
Trace . . . 346
LLC Monitoring Commands . . . 347
List . . . 347
Set . . . 347

Chapter 24. Using LAN Emulation Services . . . 349
About LAN Emulation Services . . . 349

Chapter 25. Configuring and Monitoring LAN Emulation Services . . . 351
Accessing the LAN Emulation Services Environment . . . 351
Lecs . . . 352
Les-bus . . . 352
List . . . 353
Rename . . . 353
Security . . . 354
Configuration Commands for a LES-BUS . . . 354

Add 355
Bus-filter 355
Bus-police 361
Disable 363
Enable 364
List 366
Remove 366
Set 367
Configuration Commands for a LECS 374
Access-control 374
Add 374
Database-Synchronization 375
Elans 377
List 378
Policies 378
Search 378
Set 379
Configuration Commands for the Access Control of a LECS 380
Add 381
Disable 381
Enable 381
List 381
Remove 382
Configuration Commands for ELANs at the LECS 382
Add 382
List 383
Remove 383
Select 383
Configuration Commands for ELAN Detailed Configuration 384
Les 384
List 387
Policy 387
Set 390
ELAN-TLV 390
LEC-TLV 394
Configuration Commands for the Policies of a LECS 396
Add 396
Disable 397
Enable 397
List 397
Remove 397
Configuration Commands for Security for ELANs 398
Add 398
Disable 399
Enable 399
List 399
Remove 399
Set 399
Accessing the LAN Emulation Services Monitoring Environment 400
Monitoring Commands for LAN Emulation Services 400
Create 401
Lecs 401
Les-bus 401
List 402
Security 402
Summary 403

Work . . . 403
Monitoring Commands for LES-BUS . . . 404
Bus-filter . . . 404
Bus-police . . . 411
Database . . . 413
Delete . . . 421
Disable . . . 421
Enable . . . 423
List . . . 424
Restart . . . 427
Set . . . 427
Show . . . 429
Statistics . . . 431
Stop . . . 441
Takeover . . . 441
Terminate . . . 441
Monitoring Commands for LECS . . . 442
Access-control . . . 443
Create . . . 443
Database-synchronization . . . 443
Delete . . . 445
Elans . . . 445
List . . . 445
Memory . . . 447
Policies . . . 448
Restart . . . 448
Search . . . 448
Set . . . 450
Statistics . . . 452
Monitoring Commands for the Access Control of a LECS . . . 453
Create . . . 453
Delete . . . 453
List . . . 453
Statistics . . . 454
Monitoring Commands for ELANs at the LECS . . . 454
Create . . . 455
Delete . . . 455
List . . . 455
Select . . . 456
Statistics . . . 456
Monitoring Commands for ELAN Details at the LECS . . . 457
LES . . . 457
List . . . 459
Policy . . . 460
Set . . . 461
ELAN-TLV . . . 462
LEC-TLV . . . 465
Monitoring Commands for LECS Policies . . . 466
Create . . . 467
Delete . . . 467
List . . . 467
Statistics . . . 468
Monitoring Commands for Security for LE Service . . . 469
Create . . . 469
Delete . . . 469
List . . . 470

Restart . . . 471
Statistics . . . 471

Chapter 26. Configuring and Monitoring Quality of Service (QoS) . . . 473
Quality of Service Overview . . . 473
Benefits of QoS . . . 473
QoS Configuration Parameters . . . 474
Maximum Reserved Bandwidth (max-reserved-bandwidth) . . . 474
Traffic Type (traffic-type) . . . 475
Peak Cell Rate (peak-cell-rate) . . . 475
Sustained Cell Rate (sustained-cell-rate) . . . 475
Maximum Burst Size (max-burst-size) . . . 476
QoS Class (qos-class) . . . 476
Validate PCR of Best-Effort VCCs (validate-pcr-of-best-effort-vccs) . . . 477
Negotiate QoS (negotiate-qos) . . . 478
Accept QoS Parms from LECS (accept-qos-parms-from-lecs) . . . 478
Accessing the QoS Configuration Prompt . . . 478
Quality of Service Commands . . . 479
LE Client QoS Configuration Commands . . . 480
List . . . 480
Set . . . 480
Remove . . . 484
ATM Interface QoS Configuration Commands . . . 484
List . . . 484
Set . . . 485
Remove . . . 487
Accessing the QoS Monitoring Commands . . . 487
Quality of Service Monitoring Commands . . . 487
LE Client QoS Monitoring Commands . . . 488
List . . . 488

Part 3. Appendixes . . . 493

Appendix A. Quick Configuration Reference . . . 495
Quick Configuration Tips . . . 495
Making Selections . . . 495
Exiting and Restarting . . . 495
When You're Done . . . 495
Starting the Quick Configuration Program . . . 495
Configuring LAN Emulation . . . 496
Configuring Bridging . . . 496
Configuring Protocols . . . 498
Configuring IP . . . 498
Configuring IPX . . . 500
Restarting the IBM 8210 . . . 502

Appendix B. Abbreviations . . . 505

Glossary . . . 515

Index . . . 537

Readers' Comments — We'd Like to Hear from You . . . 553

Figures

1. IBM 8210 Multiprotocol Switched Services Server 7
2. Relationship of Processes and Commands 8
3. Main Menu Panel 29
4. System Configuration Information 30
5. Test Selection Panel 32
6. Utilities Selection Panel 33
7. Set Supervisory Password Panel 34
8. Unattended Start Mode Changed (Enabled) Panel 35
9. Unattended Start Mode Changed (Disabled) Panel 36
10. Remove Supervisory Password Panel 36
11. Update System Firmware Panel 37
12. Event/Error Log Panel 38
13. View of Set Vital Product Data 40
14. Copy Remote Files Panel 41
15. Setup Remote Initial Program Load Panel 42
16. Manipulate Dead Man Timer Panel 43
17. Local Serial Connection to the EIA 232 Port 48
18. Remote Serial Connection to the PCMCIA Modem (Voice/Data/Fax Modem or Data/Fax Modem) 48
19. Connection Using IP Over the ATM Network 48
20. IBM 8210 Home Page 60
21. Configuration and Console Page 1 61
22. Diagnostic Menu 61
23. Configuration and Console Page 2 62
24. Memory Utilization 80
25. Message Generated by an Event 147
26. Syslog Message Description 153
27. syslog.conf Configuration File 155
28. Configuring the 8210 for Remote Logging 156
29. Configuring Subsystems and Events for Remote Logging 157
30. Sample Contents from Syslog News Info File 158
31. Output from Talk 2 159
32. Sample Contents from *Syslog_user_alert* File 159
33. Example of Setting Up a Static ARP Entry 160
34. Example of Recurring Sequence Numbers in Syslog Output 161
35. FDDI Network Diagram 221
36. Physical and Logical Views of a Simple LAN Emulation Network 234
37. Default Connections Between LE Clients and the LES 242
38. Default Connection Between LE Clients (LECs) and BUS 244
39. LAN Emulation Redundancy 249
40. Adding ELANs to Form a SuperELAN 257
41. Parallel SuperELANs 258
42. Redundant SuperELAN 259
43. SuperELAN II Spanning Tree 259

© Copyright IBM Corp. 1996, 1998

Tables

1. Processes, Their Purpose, and Commands to Access 10
2. Hardware Error Codes 38
3. File Transfer. 52
4. OPCON Commands. 75
5. CONFIG Command Summary 92
6. Access Permission 94
7. IBM 8210 Feature Numbers and Names 101
8. Additional Functions Provided by the Set Prompt Level Command. . . . 110
9. Default and Maximum Settings for Interfaces. 110
10. Change Management Configuration Commands 115
11. GWCON Command Summary 130
12. Logging Levels. 148
13. Packet Completion Codes (Error Codes) 148
14. ELS Configuration Command Summary 165
15. ELS Message Buffering Configuration Commands. 180
16. ELS Monitoring Command Summary 184
17. Packet Trace Monitoring Command Summary 204
18. ELS Message Buffering Monitoring Commands. 207
19. PERF Configuration Command Summary 214
20. PERF Monitoring Command Summary 215
21. FDDI Configuration Command Summary 223
22. FDDI Monitoring Command Summary 226
23. ATM Configuration Command Summary 268
24. ATM INTERFACE Configuration Command Summary 269
25. ATM Virtual Interface Configuration Command Summary 275
26. ATM monitoring command Summary. 277
27. ATM INTERFACE monitoring command Summary. 278
28. ATM LLC Configuration Command Summary 281
29. SuperELAN Configuration Command Summary. 283
30. Selected SuperELAN Configuration Command Summary 287
31. Selected ELAN Configuration Command Summary 294
32. SE Services Monitoring Command Summary 297
33. Selected SuperELAN monitoring command Summary 298
34. Selected ELAN Monitoring Command Summary 305
35. LAN EMULATION Client Configuration Commands Summary 313
36. LAN Emulation Client Configuration Commands Summary. 315
37. ATM LAN Emulation Client ARP Configuration Commands Summary. . . 316
38. ATM LAN Emulation Client ARP Config Commands Summary 317
39. IBM LAN Emulation Client Configuration Commands Summary 330
40. LLC Command Summary 336
41. LE Client Monitoring Command Summary. 338
42. LLC Monitoring Command Summary. 347
43. LAN EMULATION Services Configuration Commands Summary 352
44. LES-BUS Configuration Commands Summary 354
45. BUS Filter Configuration Commands Summary 355
46. BUS Police Configuration Commands Summary 361
47. LECS Configuration Commands Summary 374
48. LECS Database Synchronization Configuration Commands Summary . . 375
49. Access Control Configuration Commands Summary 380
50. LECS ELANs Configuration Commands Summary. 382
51. LECS ELANs Detailed Configuration Commands Summary 384
52. Selected ELAN LES Configuration Commands Summary 384
53. Selected ELAN-TLV Configuration Commands Summary 391

© Copyright IBM Corp. 1996, 1998

54. Selected LEC-TLV Identifiers Summary 395
55. Selected LEC-TLV Command Summary 395
56. LECS Policies Configuration Commands Summary 396
57. LECS Interface Configuration Commands Summary 398
58. LAN EMULATION Services Monitoring Commands Summary 400
59. LES-BUS Monitoring Commands Summary 404
60. BUS Filter Monitoring Commands Summary 404
61. BUS Police Monitoring Commands Summary 411
62. LECS Monitoring Commands Summary 442
63. LECS Database Synchronization Monitoring Commands Summary . . . 444
64. Access Control Monitoring Commands Summary 453
65. ELAN Monitoring Commands Summary 454
66. ELAN Details Monitoring Commands Summary 457
67. Selected ELAN-TLV Monitoring Commands Summary 462
68. Selected LEC-TLV Identifiers Summary 465
69. Selected LEC-TLV Command Summary 465
70. LECS Policies Monitoring Commands Summary 466
71. Security for LE Services Monitoring Commands Summary 469
72. Quality of Service (QoS) Configuration Command Summary 479
73. LE Client Quality of Service (QoS) Configuration Command Summary . . 480
74. LE Client Quality of Service (QoS) Configuration Command Summary . . 484
75. Quality of Service (QoS) Monitoring Command Summary 487
76. LE Client QoS Monitoring Command Summary 488

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785, U.S.A.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement.

This document is not intended for production use and is furnished as is without any warranty of any kind, and all warranties are hereby disclaimed including the warranties of merchantability and fitness for a particular purpose.

© Copyright IBM Corp. 1996, 1998

Notice to Users of Online Versions of This Book

For online versions of this book, you are authorized to:

- Copy, modify, and print the documentation contained on the media, for use within your enterprise, provided you reproduce the copyright notice, all warning statements, and other required statements on each copy or partial copy.
- Transfer the original unaltered copy of the documentation when you transfer the related IBM product (which may be either machines you own, or programs, if the program's license terms permit a transfer). You must, at the same time, destroy all other copies of the documentation.

You are responsible for payment of any taxes, including personal property taxes, resulting from this authorization.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Your failure to comply with the terms above terminates this authorization. Upon termination, you must destroy your machine-readable documentation.

© Copyright IBM Corp. 1996, 1998

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

Advanced Peer-to-Peer Networking	CUA	Operating System/2
AIX	IBM	RS/6000
AIXwindows	Micro Channel	System/370
APPN	NetView	VTAM
BookManager	Nways	Web Explorer
Common User Access	OS/2	PS/2

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation.

Other company, product, and service names may be trademarks or service marks of others.

© Copyright IBM Corp. 1996, 1998

Preface

This manual contains the information you will need to use the command line interface for configuration and operation of the IBM Nways Multiprotocol Switched Services (MSS) or the A-MSS Server Module, hereafter referred to as “the router,” installed on your IBM Multiprotocol Switched Services (MSS). With the help of this manual, you should be able to perform the following processes and operations:

- Configure, monitor, and use the base code on your IBM Nways Multiprotocol Switched Services (MSS) or the A-MSS Server Module
- Configure, monitor, and use the interfaces and Link Layer software supported by your the router.

Who Should Read This Manual: This manual is intended for persons who install and manage computer networks. Although experience with computer networking hardware and software is helpful, you do not need programming experience to use the protocol software.

Conventions Used in This Manual

The following conventions are used in this manual to show command syntax and program responses:

1. The abbreviated form of a command is underlined as shown in the following example:

   reload

   In this example, you can enter either the whole command (reload) or its abbreviation (rel).
2. Keyword choices for a parameter are enclosed in brackets and separated by the word or. For example:

   ```
   command [keyword1 or keyword2]
   ```

   Choose one of the keywords as a value for the parameter.
3. Three periods following an option mean that you enter additional data (for example, a variable) after the option. For example:

   time host ...

   In this example, you enter the IP address of the host in place of the periods, as explained in the description of the command.
4. In information displayed in response to a command, defaults for an option are enclosed in brackets immediately following the option. For example:

   ```
   Media (UTP/STP) [UTP]
   ```

   In this example, the media defaults to UTP unless you specify STP.
5. Keyboard key combinations are indicated in text in the following way:
   - – **Ctrl-P**

     The key combination **Ctrl P** indicates that you should press the Ctrl key and the ″P″ key simultaneously. In certain circumstances, this key combination changes the command line prompt.
   - Names of keyboard keys are indicated like this: **Enter**

© Copyright IBM Corp. 1996, 1998

MSS Server Library

The following hard copy publications are shipped with the product. The manuals in this list are also included in displayable softcopy form on the Multiprotocol Switched Services (MSS) Softcopy Library CD-ROM (SK2T-0378). This CD-ROM is shipped with initial orders for the MSS Server.

The reference cards and the safety information booklet are shipped in hard copy only and are not included on the CD-ROM.

- *Multiprotocol Switched Services (MSS) Server Installation and Initial Configuration Guide*, GA27-4140
- *IBM 8210 Nways Multiprotocol Switched Services (MSS) Server Operations Reference Card*, GX27-4017
- *Multiprotocol Switched Services (MSS) Server Module Installation and Initial Configuration Guide*, GA27-4141
- *IBM 8210 Nways Multiprotocol Switched Services (MSS) Server Module Operations Reference Card*, GX27-4018
- *8210 Multiprotocol Switched Services (MSS) Server User's Feature Removal and Replacement Guide*, GY27-0359
- *CAUTION: Safety Information - Read This First,* SD21-0030

The following publications are not shipped in hard copy, but are offered in soft copy form on the Multiprotocol Switched Services (MSS) Softcopy Library CD-ROM (SK2T-0378). All of these manuals can be separately ordered in hard copy form through your IBM marketing representative.

- *Multiprotocol Switched Services (MSS) Server Introduction and Planning Guide*, GC30-3820
- *Mulitprotocol Switched Services (MSS) Server Service and Maintenance Manual*, GY27-0354
- *Multiprotocol Switched Services (MSS) Interface Configuration and Software User's Guide*, SC30-3818
- *Multiprotocol Switched Services (MSS) Configuring Interfaces and Features Volume 1*, SC30-3819
- *Multiprotocol Switched Services (MSS) Configuring Protocols and Features Vol. 2*, SC30-3994
- *Event Logging System Messages Guide*, SC30-3682
- *User's Guide for Nways Multiprotocol and Access Services Products*, GC30-3830

Summary of Changes For Version 2.2

The following are the new functions in this release:

- LES/BUS Enhanced Redundancy
- LES/BUS Peer Redundancy
- BUS Data Packet Filtering
- LECS Database Synchronization
- LEC Persistant Data Direct VCCs
- Rapid LES/BUS Failure Detection
- Multiple LECS Configuration Requests
- LEC Fast Path support for 802.3 IP and Source Routed Packets
- MPOA support for IPX

- Additional Dynamic Reconfiguration function
- Bridging and Routing the same protocol within one device
- IPXWAN for multiple DLCIs
- IP Filter Enhancements
- IP Routing/Bridging on the same interface
- Bootp Enhancements
- DLSw Currency
- IPv4 enhancements
- OSPF currency
- New DVMRP configuration menus
- MOS-IP
- Increased number of interfaces
- Logging enhancements
- Event Logging System Enhancements
- Report CPU Utilization function
- Packet tracing for interfaces other than ATM
- Type of Service (TOS)
- Policy-based routing
- Console Usability and Command Completion Enhancements

The technical changes and additions are indicated by a vertical line (|) to the left of the change.

Editorial Changes

This edition begins a number of editorial changes to this book and the other software books that will:

- Reorganize the material
- Remove any unnecessary and redundant information
- Improve retrievability
- Add additional clarification to some information

This effort will take a number of editions. Please help us during this effort by reporting any corrections using the Reader's Comment Form in the back of the book.

Part 1. User's Guide

© Copyright IBM Corp. 1996, 1998

Chapter 1. Getting Started

This chapter shows you how to get started with using the following components related to the IBM Nways Multiprotocol Switched Services (MSS) Server Module (IBM 8210) and the IBM 8210 Multiprotocol Switched Services Server:

- Router console terminals
- Router software (IBM 8210 Multiprotocol Switched Services Server)
- Router software user interface

The information in this chapter is divided into the following sections:

- "Before You Begin"
- "Accessing the Software Using Local and Remote Consoles"
- "Discussing the User Interface System" on page 6

Before You Begin

Before you begin, refer to the following checklist to verify that your router is installed correctly.

HAVE YOU...

- Installed all necessary hardware?
- Connected the console terminal (video terminal) to the router?

  Attention: If you are using a service port-attached terminal to configure or monitor your IBM 8210 and your service terminal is unreadable, you need to change some parameters in your configuration. (See "Service Terminal Display Unreadable" in Mulitprotocol Switched Services (MSS) Server Service and Maintenance Manual.)

  Refer to your hardware documentation.
- Connected your router to the network using the correct network interfaces and cables?
- Run all necessary hardware diagnostics?

For more information on any of these procedures, refer to the *Multiprotocol Switched Services (MSS) Server Installation and Initial Configuration Guide*.

Migrating to the Current Release

Refer to the *Mulitprotocol Switched Services (MSS) Server Service and Maintenance Manual* for information about migrating to a new code level.

Accessing the Software Using Local and Remote Consoles

The router console lets you use the router user interface to monitor and change the function of the router's networking software (IBM 8210 Multiprotocol Switched Services Server). The router supports local and remote consoles.

© Copyright IBM Corp. 1996, 1998

Local Consoles

Local consoles are either directly connected by an EIA 232 (RS-232) cable, or connected via modems to the router. You may need to use a local console during the initial software installation. After the initial setup connection, you can connect using Telnet, as long as IP forwarding has been enabled. (Refer to *Multiprotocol Switched Services (MSS) Configuring Protocols and Features* for more information on enabling IP forwarding.)

When the configured router is started for the first time, a boot message appears on the screen, followed by the OPerator's CONsole or OPCON prompt (*). The * prompt indicates that the router is ready to accept OPCON commands.

Your IBM 8210 Multiprotocol Switched Services Server software may have been pre-configured at the factory. If it was, you do not need to use a local console to perform initial configuration. If, however, your IBM 8210 Multiprotocol Switched Services Server was not pre-configured at the factory, you will need to use an ASCII terminal attached to the 8210 service port to initially configure it.

Important: Garbage, random characters, reverse question marks, or the inability to connect your terminal to the 8210 service port can have many causes. The following list contains some of those causes:

- The most common cause of garbage or random characters on the service console is that the baud rate is not synchronized with the IBM 8210.

  If the IBM 8210 is set to a specific baud rate, the terminal or terminal emulator must be set to the same baud rate.

  If the IBM 8210 is set to autobaud (this is the default), press the terminal break key sequence and press **Enter**.

  A typical break key sequence for PC terminal emulators is Alt-B (refer to the terminal emulator documentation). Most ASCII terminals have a **Break** key (often used in conjunction with the **Ctrl** key).

  Refer to your hardware documentation for more information.
- Defective terminal or device (ac) grounds.
- Defective, incorrectly shielded, or incorrectly grounded EIA 232 (RS-232) cable between the terminal and the IBM 8210.
- Defective terminal or terminal emulator.
- Defective IBM 8210 system board.
- High ambient electromagnetic interference (EMI) levels.
- Power line disturbances.

(See “Service Terminal Display Unreadable” in the *Mulitprotocol Switched Services (MSS) Server Service and Maintenance Manual* .)

Once the IBM 8210 is initially configured, you will not need a local console for router operation, as long as IP is enabled.

The router software automatically handles console activity. When upgrading the software, you might have to use the local console. For information on attaching and configuring local consoles, refer to the *Multiprotocol Switched Services (MSS) Server Installation and Initial Configuration Guide*.

Remote Consoles

Remote consoles attach to the router using a standard remote terminal protocol. Remote consoles provide the same function as local consoles, except that a local console must be used for initial configuration if your IBM 8210 was not pre-configured at the factory.

Telnet Connections

The router supports both Telnet Client and Server. The remote console on the router acts as a Telnet server. The router acts as a Telnet client when connecting from the router to either another router or a host using the **telnet** command in the OPCON (*) process.

Remote Login Names and Passwords

During a remote login, the router prompts you for a login name and password. You can display the login name when logged in to the router from a remote console by using a router **status** command.

Logging In Remotely or Locally

Logging in to a local console is the same as logging in to a remote console except that you must connect to the router by starting Telnet on your host system. To log in remotely, begin at step 1. To log in locally, begin at step 3.

To log in from a remote console:

1. Connect to the router by starting Telnet on your host system. Your host system is the system to which remote terminals are connected.
2. Supply the router's name or Internet Protocol (IP) address.

   To use router names, your network must have a name server. Issue either the router name or the IP address as shown in the following example:

   ```
   % telnet brandenburg
   ```

   or

   ```
   % telnet 128.185.132.43
   ```

   At this point, it makes no difference whether you have logged in remotely or locally.
3. If you are prompted, enter your login name and password.

   ```
   login:
   Password:
   ```

   It is possible that there is a login and no password. The password controls access to the router. If a password has not been set, press the **Enter** key at the `Password:` prompt. Logins are not set automatically. For security, you can set up user names and passwords using the **add user** command in the CONFIG process. Remember to reload to activate any changes.

   Note: If you do not enter a login name and valid password within 1 minute of the initial prompt, or if you enter an incorrect password three times in succession, the router drops the Telnet connection.
4. Press the **Enter** key to display the asterisk (*) prompt.

You may have to press the **Enter** key more than once or press **Ctrl-P** to obtain the * prompt.

Once at this level, you can begin to enter commands from the keyboard. Press the **Backspace** key to delete the last character typed in on the command line. Press the **Delete** key or **Ctrl-U** to delete the whole command line entry so that you can reenter a command. See “Command Completion” on page 20 and “Command History” on page 22 for more information.

You can also use local Telnet commands on your Telnet client to close the Telnet connection.

Note: If you use a VT100 terminal, do not press the **Backspace** key, because it inserts invisible characters. Use the **Delete** key.

5. Exit the router as described in “Exiting the Router”.

Reloading the Router

Use the **reload** command to reboot the device by loading a new copy of the configuration from memory. Whenever you change a user-configurable parameter that is not dynamically configurable, you must reload the device for the change to take effect. For example:

```
* reload

The configuration has been changed, save it? (Yes or [No] or Abort)

Are you sure you want to reload the gateway? (Yes or [No]): yes
```

Exiting the Router

Return to the * prompt and use the **logout** command to close the Telnet connection. For example:

```
IP Config> exit
Config> Ctrl-P
* logout

%
```

You can also use local Telnet commands on your Telnet client to close the Telnet connection.

Discussing the User Interface System

The software (IBM 8210 Multiprotocol Switched Services Server) is a multitasking system that schedules use of the CPU among various processes and hardware devices. The router software:

- Provides timing and memory management, and supports both local and remote operator consoles from which you can view and modify the router’s operational parameters.
- Consists of functional modules that include various user interface processes, all network interface drivers, and all protocol forwarders purchased with the router.

Understanding the First-Level User Interface

The user interface to the software consists of the main menu (process) and several subsidiary menus (processes). These menus are related to the multiple levels of processes in the software.

The first level of processes consists of the OPCON and CONFIG-ONLY processes. In most cases, you will use the OPCON process to access the second level to configure or operate the base services, features, interfaces, and protocols you will run on your IBM 8210.

The second level contains processes such as Configuration (CONFIG), Console (GWCON) and Event Logging System (MONITR). You may use the OPCON commands **configuration**, **console** or **event** to access these second level processes. Alternatively, you may use the **status** command to list the second level processes and then use the **talk** *pid* command to access the second-level processes. There are processes that you cannot use in the software. See Table 1 on page 10 for an overview of the processes.

Figure 1 shows the processes and how they fit within the structure of the router software.

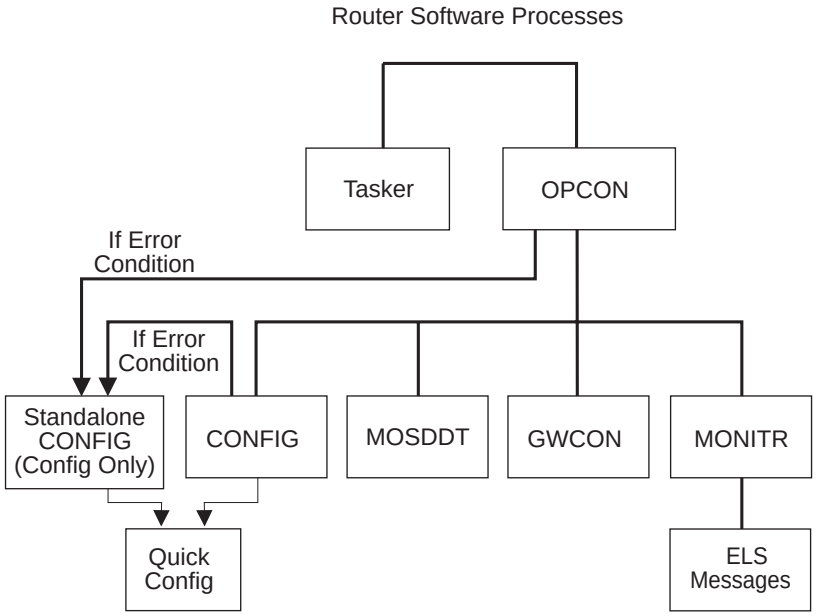


Figure 1. IBM 8210 Multiprotocol Switched Services Server

Figure 2 on page 8 is an example of the relationship between the various process levels.

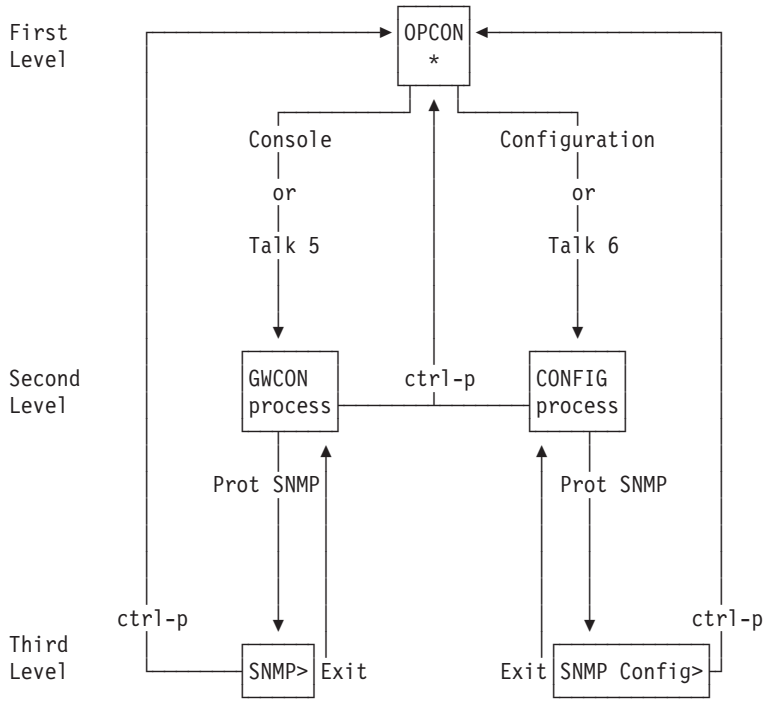


Figure 2. Relationship of Processes and Commands

Note: Also shown in Figure 2 are the various commands to access each process level and return from each process level.

See “What is the OPCON Process?” on page 75 for more information about OPCON, and “Config-Only Mode” on page 86 for more information about CONFIG-ONLY.

The ROPCON process handles processing from remote consoles and is essentially the same as the OPCON process.

Quick Configuration Process

Quick Configuration, or Quick Config, allows you to quickly configure portions of the router without dealing with the specific operating system commands. When you initially load or the router with no configuration, you enter Config-Only and you can access Quick Config menus from that process. If the router has devices configured and the devices do not have any protocols configured, the router automatically starts Config-Only and then enters Quick Config.

You can also enter Quick Config from the CONFIG process using the **qconfig** command.

System Security

Multiple users with login permissions can be added using the **add user** command. See “Configuring User Access” on page 87 for details on security issues and for information on the **set password** and **add user** commands.

Chapter 2. Using the Software

This chapter describes how to use the software. It consists of:

- "Entering Commands"
- "Connecting to a Process"
- "Some Configuration Suggestions" on page 11
- "Accessing the Second-Level Processes" on page 14
- "Accessing the Third-Level Processes" on page 16
- "Command Completion" on page 20
- "Command History" on page 22

Entering Commands

When typing a command, remember the following:

- You may type only enough sequential letters of the command to make it unique among the available commands. For example, to execute the **reload** command you must enter **rel** as a minimum. The minimum number of required characters are underlined in the command syntax chapters.
- Commands are not case-sensitive.
- Sometimes, only the first letter of the command (and subsequent options) is required to execute the command. For example, typing **s** at the * prompt followed by pressing the **Enter** key causes the **status** command to be executed.
- You may type **Escape ?** to obtain help on entering commands. See "Command Completion" on page 20 and "Command History" on page 22 for more information.

Connecting to a Process

When you start the router, the console displays a boot message. The OPCON prompt (*) then appears on the screen indicating that you are in the OPCON process and you can begin entering OPCON commands. This is the command prompt from which you communicate with different processes.

Commands that are needed more often appear before the "- - - - -" separator. Enter the appropriate command at the OPCON prompt (*). See Table 4 on page 76 for a list of commands.

Alternatively, you can:

1. Find out the process ID (PID) number of a process by entering the **status** command at the * prompt.

   The **status** command displays information about the router processes, such as the process IDs (PIDs), process names and status of the process. Issuing the **status** command is shown in the following example:

```
* status
Pid  Name      Status TTY  Comments
1    COpCON    RDY    TTY0
2    Monitr    DET     --
3    Tasker    RDY     --
```

© Copyright IBM Corp. 1996, 1998

```
4    MOSDBG    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    ELScon    DET     --
8    ROpCon    IDL    TTY1 128.185.210.125
9    ROpCon    IDL    TTY2
10   WEBCon    IDL     --
```

2. Use the **talk** *pid* command, where *pid* is the number of the process to which you want to connect. (For more information about these and other OPCON commands, refer to “What is the OPCON Process?” on page 75.)

   Note: Not every process listed has a user interface (for example, the **talk 3** process). The **talk 4** command is for use by IBM service representatives.

Identifying Prompts

Each process uses a different prompt. You can tell which process your console is connected to by looking at the prompt. (If the prompt does not appear when you enter the **talk** *pid* command, press **Enter** again.)

The following list shows the prompts for the five main processes:

Table 1. Processes, Their Purpose, and Commands to Access

Process	Level and Purpose	Command to Access	Input Prompt
OPCON	Level 1 - access to all secondary levels	**Ctrl-P**	asterisk (*)
CONFIG	Level 2 - base services configuration and access to configuration third level	**Configuration or talk 6**	Config >
GWCON	Level 2 - base services operation and monitoring and access to operations and monitoring on third level	**Console or talk 5**	plus sign (+)
MONITR	level 2 - message display	**Event or talk 2**	(none)
ELSCon	level 2 - direct monitoring and access to ELS console	**els or talk 7**	ELS Secondary Console>
MOSDBG	level 2 - diagnostic environment	**talk 4**	db>
Note: Only enter the **talk 4** command under the direction of a service representative.			

At the OPCON prompt level, you can begin to enter commands from the keyboard. Use the **Backspace** key to delete the last character typed in on the command line. Use **Ctrl-U** to delete the whole command line entry so that you can reenter a command. See “Command Completion” on page 20 and“Command History” on page 22 for additional details or press **Escape ?**.

Getting Help

At the command prompts, you can obtain help in the form of a listing of the commands available at that level. To do this, type **?** (the **help** command), and then press **Enter**. Use **?** to list the commands that are available from the current level. You can usually enter a **?** after a specific command name to list its options. For example, the following information appears if you enter **?** at the * prompt:

```
*?
        CONFIGURATION         (Talk 6)
        CONSOLE                 (Talk 5)
        EVENT Logging System  (Talk 2)
        ELS Console              (Talk 7)
        LOGOUT
        PING (IP-Address)
        RELOAD
        RESTART
        TELNET to IP-Address (this terminal type)
-----------------------------------------------
        DIVERT output from process
        FLUSH output from process
        HALT output from process
        INTERCEPT character is
        MEMORY statistics
        STATUS of Processes(es)
        TALK to process
(you may cycle through these commands by pressing the TAB key)
```

Exiting a Lower Level Environment

The multiple-level nature of the software places you in secondary, tertiary, and even lower level environments as you configure or operate the 8210. To return to the next higher level, enter the **exit** command. To get to the secondary level, continue entering **exit** until you receive the secondary level prompt (either `Config>` or `+`).

For example, to exit the IP protocol configuration process:

```
IP config> exit
Config>
```

If you need to get to the primary level (OPCON), enter the intercept character (**Ctrl P** by default).

Getting Back to OPCON

To get back to the OPCON prompt (*), press **Ctrl-P**. You must always return to OPCON before you can communicate with another process. For example, if you are connected to the console (GWCON) process and you want to connect to the CONFIG process, you must press **Ctrl-P** to return to OPCON first. The **Ctrl-P** key combination is the default *intercept character*.

If you use the intercept character from a third-level or lower level menu to return to the * prompt, the next time you use the **talk** command to talk to the same process, you will reenter that same level menu. This link goes away when the router is re-initialized.

Some Configuration Suggestions

Configuring a 8210 is different depending on whether you are configuring for the first time, creating a configuration based on an existing configuration, or just updating a configuration. Use the following sections as a guide to the best procedure to use, depending on your needs.

Creating a First Configuration

This procedure assumes that you have no other 8210 that contains a configuration similar to the one for the 8210 you are configuring. The procedure also assumes

that you have just taken the 8210 out of the box. Although this procedure specifies an order, you can perform the actual configuration (after step 3) in any order.

To configure a IBM 8210 for the first time:

1. Examine the 8210 you are configuring to determine which interfaces you need to configure. Note these for later use.
2. Connect to the 8210 as described in “Accessing the Software Using Local and Remote Consoles” on page 3.
3. Initially configure a port on the 8210 and at least an internal IP address for the device using Quick Config as described in “Quick Configuration” on page 86 or “Appendix A. Quick Configuration Reference” on page 495. Configure the minimum needed to allow you to Telnet into the device.
4. Configure any base services, such as boot options. Access the configuration process as described in “Accessing the Configuration Process, CONFIG (Talk 6)” on page 14.
5. Configure the interfaces. Access the interface configuration process as described in “Accessing the Network Interface Configuration Process” on page 16.
6. Configure any required features. Access the feature configuration process as described in “Accessing Feature Configuration and Operating Processes” on page 17.
7. Configure any protocols that will run through this device. Access the protocol configuration process as described in “Accessing Protocol Configuration and Operating Processes” on page 18.

   Note: At the very least, you will configure IP in this step.
8. Reload the router as described in “Reloading the Router” on page 6.

Basing a Configuration on an Existing Configuration

This section describes how to:

- Base a configuration on the configuration in an operating 8210
- Permanently update the configuration in a 8210
- Temporarily update the configuration of a 8210 while the 8210 is operating

Basing on an Existing Configuration

If you already have a 8210 that has the same interfaces, features, and protocols that you want to configure on a new 8210, you can save time by basing the configuration on the existing 8210. You can perform this type of configuration either using the command line interface or by using the configuration program that comes with the 8210. In both cases, the procedures assume that the 8210 is not in your production network.

To base a configuration on an existing configuration using the command line interface:

1. Obtain a copy of the configuration you want to use.
   a. Enter **talk 6** at the OPCON (*) prompt.
   b. Enter **boot** at the `Config>` prompt.

c. Enter the **copy configuration** *file* command at the `Boot config>` prompt. See “Chapter 9. Using BOOT Config to Perform Change Management” on page 113 for more information.

2. Connect to the 8210 that you are configuring.
3. Load the configuration you obtained in step 1 on page 12 into the 8210 using TFTP GET. See “Chapter 9. Using BOOT Config to Perform Change Management” on page 113.
4. Update the configuration.
5. Write the configuration. See “What is CONFIG?” on page 85.
6. Reload the 8210.

To base a configuration on an existing configuration using the configuration program:

1. Start the configuration program.
2. Retrieve the configuration from the 8210 on which you want to base the new configuration.
3. Make the changes you need for the new configuration. These changes include addresses, the host names, users, and other items.
4. Save the configuration with a different name from the name that you used to retrieve the configuration.
5. Send the configuration to the 8210 you are configuring.
6. Reload the 8210.

For more about using the configuration program, see *User’s Guide for Nways Multiprotocol and Access Services Products* GC30-3830.

Permanently Updating a Configuration

To permanently update a configuration:

1. Access the 8210 you are updating as described in “Accessing the Software Using Local and Remote Consoles” on page 3. You will see the `*` prompt.
2. Enter the **talk 6** command to access the configuration process.
3. Enter the appropriate commands to access the third-level process that configures the areas that you are changing.
4. Enter **exit** as many times as needed to return to the configuration process.
5. Write the configuration. See “What is CONFIG?” on page 85.
6. Reload the 8210.

Temporarily Updating a Configuration

The ability to temporarily update a configuration allows you to make changes to some of the operating characteristics of a 8210 until you can make permanent updates to the configuration. This enables you to implement changes immediately to resolve problems or improve performance and avoid an outage during a peak period. You can then make permanent updates to the configuration and schedule an outage so you can reload to pick up the change.

To temporarily update a configuration:

1. Access the 8210 you are updating as described in “Accessing the Software Using Local and Remote Consoles” on page 3. You will see the `*` prompt.

2. Enter the **talk 5** command to access the operating/monitoring process.

   Note: Not all interface types, protocols, or features allow you to make temporary config changes via talk 5 commands.
3. Enter the appropriate commands to access the third-level process that monitors the areas that you are changing.
4. Enter **exit** as many times as needed to return to the operating/monitoring process.
5. Enter **Ctrl-P** to return to the * prompt.
6. Exit the router as described in "Exiting the Router" on page 6

Accessing the Second-Level Processes

All interfaces, features, and protocols have commands that you use to access the following processes:

- The configuration process to initially configure and enable the interface, feature, or protocol, as well as perform later configuration changes.
- The operating/monitoring process to display information about each interface, feature, or protocol, to make temporary configuration changes, or to activate configuration changes.

You can also configure or operate some base system services through the second-level processes. The commands to perform these functions are described starting in "What is CONFIG?" on page 85.

The next sections describe the procedures for accessing the second-level processes.

Accessing the Configuration Process, CONFIG (Talk 6)

Each protocol configuration process is accessed through the router's CONFIG process. CONFIG is the second-level process of the router user interface that lets you communicate with third-level processes. Protocol processes are examples of third-level processes.

The CONFIG command interface is made up of levels of menus. Protocol configuration command interfaces are menus within the CONFIG interface. Each protocol configuration interface has its own prompt. For example, the prompt for the SNMP protocol command interface is `SNMP config>`.

The next sections describe these procedures in more detail.

Entering the CONFIG Process

To enter the CONFIG process from OPCON and obtain the CONFIG prompt, enter the **configuration** command. Alternatively, you can enter the OPCON **talk** command and the PID for CONFIG. The PID for CONFIG is 6.

```
* configuration
```

or

```
* talk 6
```

The console displays the CONFIG prompt (`Config>`). If the prompt does not appear, press the **Enter** key again.

Quick Configuration Process: Quick Configuration, or Quick Config, allows you to quickly configure portions of the router without dealing with the specific operating system commands. You enter the Quick Config menus from the CONFIG process using the **qconfig** command (see "Quick Configuration" on page 86).

Reloading the Router

Changes that you make to the protocol parameters through CONFIG do not take effect until you either activate the net that contains any dynamic changes or the router software.

Accessing the Console Operating/Monitoring Process, GWCON (Talk 5)

To view information about the interfaces, features, or protocols or to change parameters while running, you must access and use the operating (monitoring) process. Operating command interfaces are modes of the GWCON interface. Within the GWCON mode, each interface, feature, or protocol interface has its own prompt. For example, the prompt for the SNMP protocol is `SNMP>`.

Note: Any parameters you change in this process will not remain active across any event that causes the 8210 to reload the operational code, such as a power outage or entering the **reload** command.

The next sections describe these procedures in more detail.

Entering the GWCON Command Process

To enter the GWCON process from OPCON and obtain the GWCON prompt, enter the **console** command. Alternatively, you may enter the **talk** command and the PID for GWCON. The PID for GWCON is 5. For example:

```
* console
```

or

```
* talk 5
```

The GWCON prompt (+) then displays on the console. If the prompt does not appear, press **Enter** again.

Accessing the Secondary ELS Console Process, ELSCon (Talk 7)

The Secondary ELS Console provides convenient access to GWCON `talk 5` ELS without disrupting the current state of GWCON. You may be in the middle of a **ping** in `talk 5`, or deep inside a `talk 5` menu structure, and want to control ELS without disrupting the current state of GWCON. The secondary ELS console (Talk 7) serves this purpose.

To enter the Secondary ELS Console (ELScon) process from OPCON and obtain the Secondary ELS Console prompt, enter the **els** command. Alternatively, you may enter the **talk 7** command.

In the following example, another ELS event is displayed while performing a **ping** command.

Note: The intercept character (Ctrl-P by default) is used to obtain the OPCON prompt (*).

```
*talk 5
+protocol ip
IP>ping 10.0.0.9
PING 10.0.0.2 -> 10.0.0.9: 56 data bytes, ttl=64, every 1 sec.

*talk 7

ELS Secondary Console>display event ip.7
Complete
ELS Secondary Console>
*talk 2
00:20:48   IP.007: 10.0.0.2 -> 10.0.0.9
00:20:49   IP.007: 10.0.0.2 -> 10.0.0.9
```

Accessing the Third-Level Processes

After accessing the second level, you must enter commands on the third level to configure or operate the interfaces, features, and protocols in your IBM 8210. The following sections describe how to access the third level processes.

Accessing Network Interface Configuration and Operating Processes

This section describes how to get started with accessing the network interface configuration and operating processes. Accessing these processes lets you change and monitor software-configurable parameters for network interfaces used in your router.

Accessing the Network Interface Configuration Process

Use the following procedure to access the router's configuration process. This process gives you access to a specific interface's *configuration* process.

1. At the OPCON prompt, enter the **configuration** command.

   ```
   * configuration
   ```

   After you enter the **configuration** command, the CONFIG prompt (`Config>`) displays on the console. If the prompt does not appear when you first enter **configuration**, press **Enter** again.

   Use the **add device** command to create a network interface. The **add device** command automatically assigns the interface number.

2. At the `Config>` prompt, enter the **list devices** command to display the network interface numbers for which the device is currently configured, as follows:

   ```
   Config> list devices

   Ifc 0 CHARM ATM Adapter          Slot: 1  Port: 1
   ```

3. Record the interface numbers.
4. Enter the CONFIG **network** command and the number of the interface you want to configure. For example:

   ```
   Config> network 1
   ```

   The appropriate configuration prompt (such as `Eth Config>` for Ethernet), now displays on the console.

Note: Not all network interfaces are user-configurable. For interfaces that cannot be configured, you receive the message:

```
That network is not configurable
```

Configuring the Network Interface: Refer to the specific chapters in this guide for complete information on configuring your IBM 8210's network interfaces.

The MSS Client supports a 155 Mbps ATM interfaces.

Accessing the Network Interface Console Process

To monitor information related to a specific interface, access the interface console process by using the following procedure:

1. At the OPCON prompt, enter the **console** command . For example:

   ```
   * console
   ```

2. The GWCON prompt (+) is displayed on the console. If the prompt does not appear when you first enter GWCON, press **Enter** again.
3. At the GWCON prompt, enter the **configuration** command to see the protocols and networks for which the router is configured. For example:

   ```
   + configuration

   Nways 8210 Multiprotocol Switching Server
   Host name: [not configured]
   Version: 1.0

   Num Name  Protocol
   0   IP    DOD-IP
   3   ARP   Address Resolution
   11  SNMP  Simple Network Management Protocol
   12  OSPF  Open SPF-Based Routing Protocol
   23  ASRT  Adaptive Source Routing Transparent Enhanced Bridge

   Num Name  Feature
   2   MCF   MAC Filtering
   6   QOS   Quality of Service

   3 Networks:
   Net Interface  MAC/Data-Link         Hardware         State
   0   ATM/0      ATM                   CHARM ATM        Up
   ```

4. Enter the GWCON **network** command and the number of the interface you want to monitor. For example:

   ```
    + network 0
   ATM>
   ```

   In this example, the ATM console prompt is displayed on the console. You can then view information about the ATM interface by entering the ATM console commands.

Monitoring the Network Interface: Refer to the specific chapters in this manual for complete information on monitoring your IBM 8210's network interfaces.

Accessing Feature Configuration and Operating Processes

To help you access the IBM 8210 Multiprotocol Switched Services Server feature configuration and operating processes, this section outlines both of these procedures.

Accessing the Feature Processes

Use the **feature** command from the CONFIG process to access configuration commands for specific IBM 8210 Multiprotocol Switched Services Server features outside of the protocol and network interface configuration processes.

Use the **feature** command from the GWCON process to access console commands for specific features that are outside of the protocol and network interface console processes.

Enter a question mark after the **feature** command to display a listing of the features available for your software release. For example:

```
Config> feature ?

QOS
MCF

Feature name or number [2] ?
```

To access a particular feature's configuration or operating prompt, enter the **feature** command at the Config> or + (GWCON) prompt, respectively, followed by the feature number or short name. For example:

```
Config> feature mcf

MAC filtering user configuration

Filter Config>
```

Table 7 on page 101 lists the available feature numbers and names.

Once you access the configuration or operating prompt for a feature, you can begin entering specific commands for the feature. To return to the previous prompt level, enter the **exit** command at the feature's prompt.

Accessing Protocol Configuration and Operating Processes

This section describes how to access the protocol configuration and operating processes.

Entering a Protocol Configuration Process

To enter the desired protocol configuration process from the CONFIG> prompt:

1. At the CONFIG> prompt, enter the **list configuration** command to see the numbers and names of the protocols purchased in your copy of the software. See page 102 for sample output of the **list configuration** command.
2. From the Config> prompt, enter the **protocol** command with the number or short name (for example, SNMP) of the protocol you want to configure. The protocol number and short name is obtained from the **list configuration** command display. In the following example, the command has been entered for accessing the SNMP protocol configuration process:

   ```
   Config> protocol SNMP
   ```

   or

   ```
   Config> protocol 11
   SNMP user configuration
   ```

The protocol configuration prompt then displays on the console. The following example shows the SNMP protocol configuration prompt:

```
SNMP config>
```

You can now begin entering the protocol's configuration commands. See the corresponding protocol section of the *Multiprotocol Switched Services (MSS) Configuring Protocols and Features* for more information on specific protocol configuration commands.

In summary, the **protocol** command lets you enter the configuration process for the protocol software installed in your router. The **protocol** command enters a protocol's command process. After entering the protocol command, the prompt of the specified protocol appears. From the prompt, you can enter commands specific to that protocol.

Entering a Protocol Operating Process

To enter a protocol console process from the GWCON prompt:

1. At the GWCON prompt, enter the **configuration** command to see the protocols and networks configured for the router. For example:

```
+configuration

  Nways 8210 Multiprotocol Switching Server
Host name: NCE #2
Version:  16.0[R1]

Num Name  Protocol
0   IP    DOD-IP
3   ARP   Address Resolution
7   IPX   Netware IPX
11  SNMP  Simple Network Management Protocol
12  OSPF  Open SPF-Based Routing Protocol
23  ASRT  Adaptive Source Routing Transparent Enhanced Bridge

Num Name  Feature
2   MCF   MAC Filtering
6   QOS   Quality of Service

6 Networks:
Net Interface  MAC/Data-Link         Hardware           State
0   ATM/0      ATM                   CHARM ATM          Up
1   ATM/1      ATM                   CHARM ATM          Up
2   TKR/0      Token-Ring/802.5      CHARM ATM          Up
3   Eth/0      Ethernet/IEEE 802.3   CHARM ATM          Up
4   TKR/1      Token-Ring/802.5      CHARM ATM          Up
5   Eth/1      Ethernet/IEEE 802.3   CHARM ATM          Down
```

2. Enter the GWCON **protocol** command with the protocol number or short name of the desired protocol displayed in the configuration information.

   In the following example, the command has been entered for accessing the SNMP protocol console process.

```
+ protocol 11
```

   or

```
+ protocol SNMP
```

   The protocol console prompt then displays on the console. This example shows the SNMP protocol console prompt:

```
SNMP>
```

You can now begin entering the protocol's commands. See the corresponding protocol section of the *Multiprotocol Switched Services (MSS) Configuring Protocols and Features* for more information on specific protocol console commands.

Command Completion

The automatic command completion function assists you with the syntax for commands entered at the command line.

To illustrate the behavior of Command Completion, assume that the following commands are allowed in a given menu context. (This is an example menu only.)

enable
    auto-refresh
    caching

set cache-size
    cache-timeout
    priority

- If you type **ena** and hit the Space Bar, the full command is shown as **ENABLE**. If you now type **?**, a list of possible items to enable are shown (**auto-refresh** and **caching**) and the command **ENABLE** remains on the command line.
- If you type **ena** and press **Enter**, a message is printed that the command is not fully specified, and a list of possible items to enable are shown (**auto-refresh** and **caching**) and the command **ENABLE** remains on the command line.
- Since the **ENABLE** command requires an item to enable, it appears in a list of possible command completions with "..." in the left margin to indicate that more input is required for the command.
- If your input matches multiple commands, a list of possible completions is displayed. Your input on the new command line is expanded to the longest common prefix. For example, if you enter **set ca**, and then press the space bar, **CACHE-SIZE** and **CACHE-TIMEOUT** will be listed, and the new command line will be expanded to **SET cache-**, since "cache-" is common to both possible completions. Now you must type the letter "s" or the letter "t" to distinguish between the possible completions ″size″ or ″timeout″.
- Common commands sometimes appear in an alternate form (**SHOW**, **DISPLAY**, **LIST**). If the Command Completion does not yield a match on a common command, such as **SHOW**, the alternatives **DISPLAY** or **LIST** will be displayed, if found.
- If the search for a command (and alternatives) does not yield an exact match, you are presented with a list of possible completions, using some portion of your input. For example, **enanle** followed by the Space Bar would be replaced with **ena** and **ENABLE** would be listed as the possible completion.
- When a list of possible commands is shown, you can use the Tab key to cycle through one command at a time on the current command line. You can use the Space Bar or Enter key to select the command shown.

Online Help When Command Completion is Enabled

The following online help is available when command-completion is enabled.

See 99 for the **enable command-completion** syntax.

? Question mark displays a list of possible completions. A message appears if the command is already complete.

Space bar
Attempts to complete the current word on the command line. If a unique match is not found, possible completions are listed.

Tab Attempts to complete the current word on the command line. If a unique match is not found, possible completions are listed and you may cycle through these possible completions using the Tab key. Use the Space Bar or the Enter key to select the currently displayed command.

Enter Attempts to complete the current word on the command line. If the command is complete, Enter executes the command and stores it in the Command History. If the command is incomplete, a list of possible completions is displayed.

Ctrl-P Returns to the MOS Operator Console prompt (*). (CTL-P is the default Intercept Character.)

Backspace
Deletes the last character on the command line.

Ctrl-W Deletes the last word on the command line.

Ctrl-U Aborts the current command.

Ctrl-L Refreshes the current command line to display its contents.

Ctrl-B Retrieve Backward. Replaces the current command line with the previous command in the circular Command History.

Ctrl-F Retrieve Forward. Replaces the current command line with the next command in the Command History.

Ctrl-R Marks the start of a Repeat Sequence in the Command History. Use with the **Ctrl-N** function.

Ctrl-N Replaces the current command line with the next command in the Repeat Sequence whose starting command was marked with **CTL-R**.

Ctrl-C Cancels Easy-Start, if active.

Escape ?
Escape, followed by "?" prints this Command Line Help:

The following rules apply to automatic command completion:

- Completed commands are shown in UPPERCASE on the command line.
- Common commands sometimes appear in an alternate form (**ADD** versus **CREATE**). If the command completion does not yield a match on a common command, any alternative commands will be displayed.
- If the search for a command (and alternative commands) does not yield a unique match, a list of possible completions is shown, and the longest common prefix is presented.
- When possible completions are listed, commands requiring further command input are shown with "..." in the left margin.
- When a Command History retrieve key (CTL-B,F,N) is pressed, the Command History is scanned for a command that successfully parses in the current command context. A tone will be sounded if no such command exists.
- Some command menus are built dynamically. Command Completion cannot always follow these dynamic links. '?' can be entered in these cases.

- To disable Command Completion for just one command (to enter a comment), type any Comment Character as the first character on the command line. The Comment Characters are !@#$%*:;/'"
- Command Completion will be disabled in the event of an internal error. Report the Debug information on the screen to Customer Support.
- Command Completion is currently Enabled. To Disable this option, use the **disable command-completion** command from Configuration `talk 6`.

Online Help When Command Completion is Disabled

The following online help is available when command-completion is disabled:

? When a '?' (Question Mark) is entered at the end of the command line, a list of possible completions is shown.

Enter Executes the command and stores it in the Command History. A message is printed if the command is not fully specified

Ctrl-P Returns to the MOS Operator Console prompt (*). (CTL-P is the default Intercept Character.)

Backspace
Deletes the last character on the command line.

Ctrl-U Aborts the current command.

Ctrl-B Retrieve Backward. Replaces the current command line with the previous command in the circular Command History.

Ctrl-F Retrieve Forward. Replaces the current command line with the next command in the Command History.

Ctrl-R Marks the start of a Repeat Sequence in the Command History. Use with the **Ctrl-N** function.

Ctrl-N Replaces the current command line with the next command in the Repeat Sequence whose starting command was marked with **CTL-R**.

Ctrl-C Cancels Easy-Start, if active.

Escape ?
Escape, followed by "?" prints this Command Line Help:

•

```
Command Completion is currently Disabled.  To Enable this option,
use the enable command-completion command from Configuration talk 6.
```

Command History

The Command History contains up to the last 50 commands entered by the user in OPCON, GWCON (Talk 5) or CONFIG (Talk 6) command line menus.

Backward and Forward retrieve keys can be used to recall previously entered commands. In addition, a facility is provided to enable the advanced user to repeat a particular series of commands.

Repeating a Command in the Command History

By pressing **Ctrl-B** (backward) or **Ctrl-F** (forward) at any command line prompt in an OPCON, GWCON or CONFIG menu, the current command line is replaced by the previous or next command in the Command History. The Command History is common across the command line interface. That is, a command entered while in a GWCON menu can be retrieved from within CONFIG and a command entered while in a CONFIG menu can be retrieved from within GWCON.

When automatic Commmand Completion is enabled (See“Command Completion” on page 20) and a Command History retrieve key (CTL-B,F,N) is pressed, the Command History is scanned for a command that successfully parses in the current command context. A tone will be sounded if no such command exists.

The Command History contains the most recently entered commands, up to a maximum of the last 50 commands. If only three commands have been entered since a restart, pressing **Ctrl-F** or **Ctrl-B** circles through only those three commands. If no commands have been entered thus far, **Ctrl-F** or **Ctrl-B** results in tone sound.

Note: A command aborted by pressing **Ctrl-U** will not be entered into the Command History. When Command Completion is enabled, only complete commands are entered into the Command History.

To enter two similar commands:

```
display sub les
display sub lec
```

Enter:

`display sub les`, then press **Enter**

Ctrl-B for Backward, and the current line is replaced with-

`display sub les`

Press **Backspace** and replace “s” with “c” to get

`display sub lec` and then press **Enter**

Repeating a Series of Commands in the Command History

There is an additional feature for advanced users to facilitate repeating a particular series of GWCON or CONFIG commands. C1, C2,...,Cn in the Command History is referred to as a *repeat sequence*. This feature may be more convenient than simply using **Ctrl-B** and **Ctrl-F** when you must repeat a given task that requires multiple commands. Enter **Ctrl-R** (repeat) to set the start of the *repeat sequence* at command C1. Enter **Ctrl-N** (next) successively to retrieve the next command(s) in the repeat sequence. Commands are not automatically entered, but are placed on the current command line allowing you to modify or enter the command.

To produce the desired behavior of a repeat sequence, the first command retrieved using the first **Ctrl-N** (next) depends on the manner in which the start of the repeat sequence was set using **Ctrl-R** (repeat).

Setting the start of the repeat sequence with **Ctrl-R** can be done in two ways:

1. When C1 is initially entered
2. When C1 is retrieved from the Command History with **Ctrl-B** or **Ctrl-F**.

Starting a Repeat Sequence As Commands Are Entered

If you enter **Ctrl-R** as command C1 is being keyed in, and then enter commands C2, C3... Cn. **Ctrl-N** will successively bring commands C1, C2, ... Cn, C1, C2, ... Cn, C1, ... to the command line.

In Example 1, the start of the repeat sequence is set as the first command is keyed in. The user knows ahead of time that the same commands to be entered in GWCON need to be repeated in CONFIG.

Example 1

1. As the first command in the sequence is keyed in, use **Ctrl-R** (repeat) to set the start of the repeat sequence.

   ```
   *console
   +event Ctrl-R
   ```

   then press **Enter** to set the start of the repeat sequence.
2. Continue typing the subsequent commands in the sequence:

   ```
   Event Logging System user console
     ELS>display sub les
     ELS>display sub lec
     ELS>exit
     +
   ```
3. To enter these same commands in CONFIG, press

   Ctrl-P (the default OPCON intercept character) and go to CONFIG.

   ```
   +-press Ctrl-P-
   *configuration
   Config>Ctrl-N for NEXT to retrieve the start of this sequence-
   Config>event Enter
   Event Logging System user configuration
   ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
   ELS config>display sub les Enter
   ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
   ELS config>display sub lec Enter
   ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
   ELS config>exit Enter
   Config>
   ```

Starting a Repeat Sequence After All Commands Are Entered

On the other hand, if you first enter C1, C2, ... Cn, and retrieve C1 via **Ctrl-B** or **Ctrl-F**. Entering **Ctrl-R**, entering **Ctrl-N** successively brings commands C2,..., Cn, C1, C2,..., Cn, C1,...,Cn to the command line (see Example 2). The first occurrence of C1 is bypassed since C1 is already available on the command line at the time it was retrieved, and does not need to be recalled again by the first **Ctrl-N**.

In Example 2, all the commands are entered and then the first command in the sequence to be repeated is retrieved. A sequence of commands has been entered in GWCON, and the same sequence needs to be repeated in CONFIG.

Example 2

1. Enter the following commands in GWCON:

   ```
   *console
   +event
   Event Logging System user console
   ```

```
ELS>display sub les
ELS>display sub lec
ELS>exit
+
```

2. To enter these same commands in CONFIG, press **Ctrl-P** (the default OPCON intercept character) and go to CONFIG.

```
+Ctrl-P-
*configuration
Config>Ctrl-B four times to retrieve the start of
        the four command sequence in this example-
Config>event
Config>event Ctrl-R for REPEAT to set the start of the repeat sequence-
 Config>event Enter
 Event Logging System user configuration
 ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
 ELS config>display sub les Enter
 ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
 ELS config>display sub lec Enter
 ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
 ELS config>exit Enter
 Config>
```

Chapter 3. Using MSS Server Firmware

The MSS Server contains firmware that tests the hardware each time the MSS Server is powered on. If the MSS Server has not loaded its operational code, the firmware will be running.

One of the functions is to perform hardware checking after a power-on, and decide which version of the operational code will be loaded. It also allows you to change some of the hardware-related parameters, and manage the operational code and your configuration files.

The System Management Services menu appears when the MSS Server is set up to boot up in “Attended Mode.”

Important:

1. You can also access the firmware by stopping the boot process. To do this, you must have a TTY console directly attached to the EIA 232 service serial port. When the server starts its boot process, press and hold **Ctrl-C** or **F1** at the terminal keyboard.
2. If the firmware panels do not appear after you complete the above step:
   a. Be sure that your workstation is connected to the EIA 232 service serial port on the server.
   b. Reset or power down and power up the server.
3. You can use the up(↑) and down arrow (↓) keys or the Tab key to move around the firmware panels.

Accessing the Firmware Prompt

Before booting the server, note that:

- You will need a terminal or IP workstation connected to the server. This can be a VT100 TTY device connected directly through the serial port.

Important: To access the Firmware prompt, you can stop the MSS Server boot. To stop it, you must have a TTY console directly attached to the serial port. When the MSS Server starts its boot sequence, press **Ctrl-C** from the console to interrupt the boot sequence.

Another way to control booting is to configure the MSS Server to come up in Attended mode. Attended mode can be configured from the Firmware command set.

Boot Options Available for the MSS Server

The MSS Server can be configured for Unattended mode. In Unattended mode, you must have chosen which load image and which configuration to load. You are provided with two or three banks to choose from.The structure of the image banks is as follows:

- IMAGE - Status of image
- CONFIG 1 - Status of Config
- CONFIG 2 - Status of Config
- CONFIG 3 - Status of Config

© Copyright IBM Corp. 1996, 1998

- CONFIG 4 - Status of Config

See “List” on page 121 for a description of file statuses.

Attended Mode

When the server is configured to come up in attended mode, you have access to the Firmware System Management Services.

Connection in attended mode is through a TTY connection. You can transfer files using the Xmodem protocol for TTY or TFTP for IP connections.

In attended mode, you can start booting the server by pressing **F9** or by pressing **Ctrl+A**, then **9**, and then **Enter** to start the operating system. The system will prompt you to enter the supervisory password. The default password is **mss**.

Unattended Mode

This is the normal mode for the 8210. It will come up on the Active, Local, or Pending image and config based on your choice.

A password is not required to boot up in unattended mode.

Starting the MSS Server Firmware

You can begin using the information in this section after you have prepared your service terminal and have established connection with the server.

From the Main Menu panel (as shown in Figure 3 on page 29), you can select one of four services. The following sections explain these services and provide instructions for going through the associated panels:

- “Managing the Configuration” on page 29
- “Selecting the Boot Sequence” on page 30
- “Selecting a Device To Test” on page 30
- “Using the Utilities” on page 32

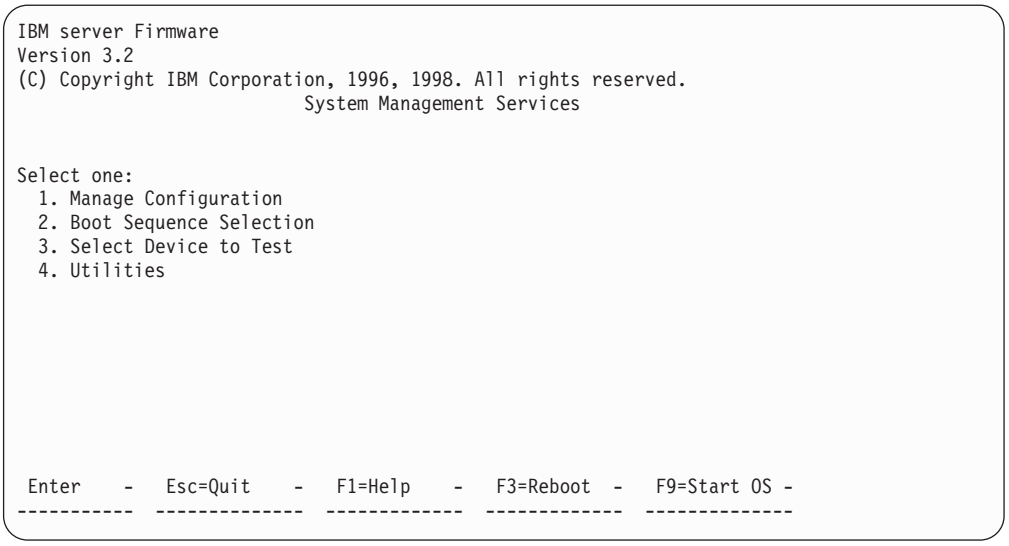


Figure 3. Main Menu Panel

The Function Keys

As seen in Figure 3, various function keys appear at bottom of the panels. These keys are common among the MSS Server Firmware panels. On other panels the functions keys are stacked at the right of the panel. Use the F1 Help key to get descriptions for the function keys associated with the MSS Server Firmware.

If your terminal does not support function keys, use the key combination, **Ctrl A** # to emulate the function keys.

Note: With some terminal emulators, you may need to define the keys as follows:

Key	Definition
F6	^[[006q
F9	^[[009q

Obtaining Help

Online helps are available for panels whenever the F1 key appears at the lower portion of the panel. Pressing F1 presents a pop-up help window with information relating to the currently active panel.

Managing the Configuration

Managing the configuration involves defining and modifying some configuration values. You can change the operational parameters for the EIA 232 service serial port and the PCMCIA modem by pressing the F6 Modify key.

Note: Although you can modify the speed, parity, data bits, and so on, of either the EIA 232 service serial port or the PCMCIA modem, it is recommended that you modify only the PCMCIA modem and not the EIA 232 service serial port.

1. Select **1. Manage Configuration** from the main menu as shown in Figure 3.

2. The *System Configuration Information* panel appears as shown in Figure 4 .

   Note: Only the fields under Serial Ports can be changed (modified). To change the specifications for a port, move the cursor to the field, press **F6**, and type in the new value.

   Use the down arrow (↓) key to scroll to the next panel.

3. Press **Enter** to make the change effective.
4. To display serial ports, press **F6** after selecting the processor type.

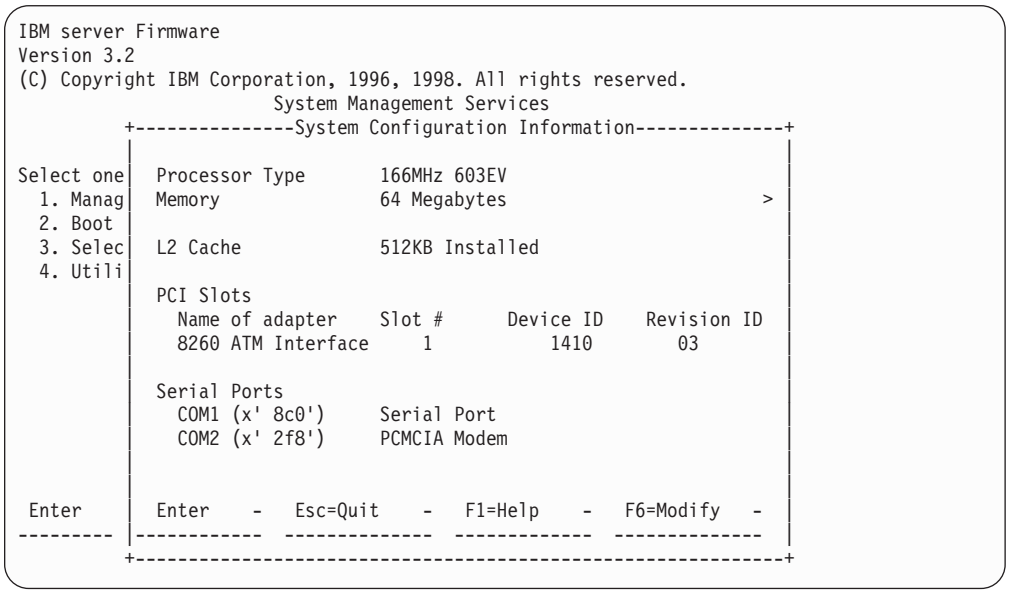


Figure 4. System Configuration Information

Selecting the Boot Sequence

This function enables you to select a sequence for the various boot devices, display the current boot device settings, restore the default setting, and boot from other boot devices.

Attention: It is not recommended that you use this function. Use the Change Management option under the Utilities menu instead. See “Chapter 9. Using BOOT Config to Perform Change Management” on page 113 for more information about change management.

Selecting a Device To Test

The firmware performs hardware tests when the MSS Server boots up. But there may be times when you have removed and replaced a failing part and you want to run an individual test before a full boot up or reset. The firmware allows you to run these individual tests:

- Test All Subsystems: This test runs all the subsystem tests that are listed on this panel.

  Note: This list is a variable list and the entries are based on diagnostic files.
- Test Memory: This test searches all available memory regions, tests the regions, and presents a consolidated list of test results.
- Test System Board: This tests the PowerPC CPU, the System Board interrupts, the PCMCIA controller, the system board temperature sensor and its interrupt mechanism, and turns the LEDs on and off (you must visually confirm that the LEDs are indeed on or off).
- Test 8260 Mailbox: This tests the Mailbox communications interface with the 8260 or 8265.
- Test IDE Devices: This tests the IDE hard drive devices
  - Device self test
  - Read/Seek test
  - Buffer test

  It also allows low-level formatting of the hard drive.

  Note: Perform low-level formatting only under the guidance of service support personnel.
- ATM Interface to Hub: This tests the ATM subsystem in the A-MSS Server Module.
- 155-Mbps ATM Adapter: This tests the ATM adapter and allows the testing of the physical interface in the MSS Server when used with an optical wrap plug.
- FDDI Adapter: This tests the FDDI adapter in the MSS Server.

To test a device:

- Select **3. Select Device to Test** from the main menu.

  The *Select Device to Test* panel appears (Figure 5 on page 32).

  Note: The *Select Device to Test* panel is created dynamically, depending on what diagnostics have been loaded. What items appear depend on whether you have an MSS Server or an A-MSS Server Module.

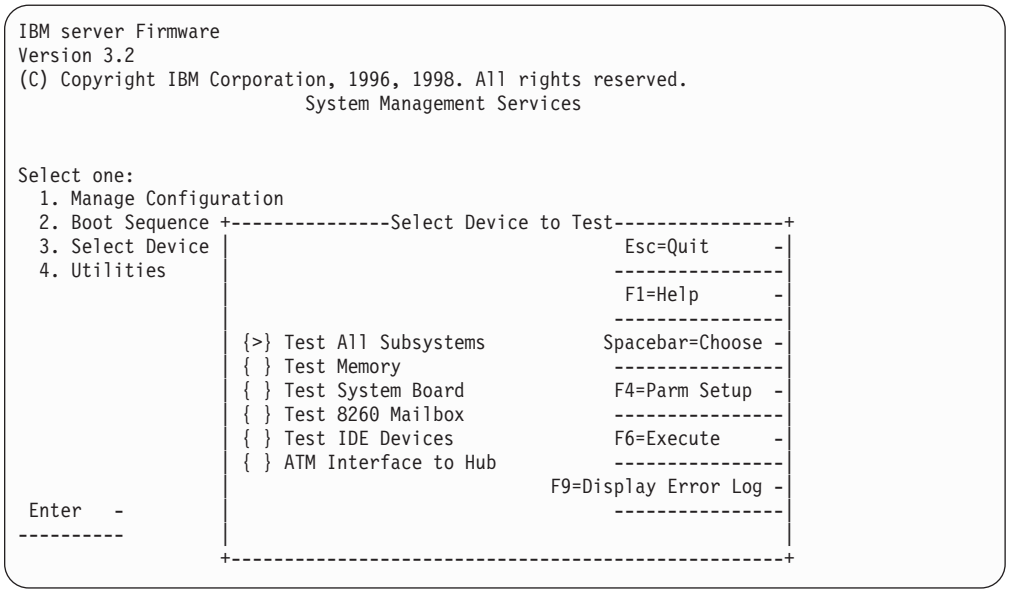


Figure 5. Test Selection Panel

- Use the spacebar and up arrow and down arrow keys to select the test that you want to run.
- Move the cursor to a selection and press **F4** to define additional test parameters.

  Note: Errors encountered during diagnostics are logged in the hardware error log.
- The *Test Parameters* panel appears. From this panel you can select:
  - Run Interactive Test
  - Run Wrap Tests
  - Stop On Error
  - Loop Tests
  - Loop Count

  Press **Esc** to return to the *Select Device Test* panel.
- Press **F6** to start a test.
- After the test is complete, press **Esc** to return to the main menu panel.

The adapter diagnostics are stored on the hard drive in the MSS Server. These diagnostics can be installed by using the “Copy Remote Files” utility and storing the file in the C:\DIAGS directory. The file extension of the adapter diagnostics is .6DG.

Using the Utilities

To use the utilities:

1. Select **4. Utilities** from the main menu.

   A panel listing the available utilities appears (Figure 6 on page 33).

```
IBM server Firmware
Version 3.2
(C) Copyright IBM Corporation, 1996, 1998. All rights reserved.
                            System Management Services


Select one:
  1. Set Supervisory Password
  2. Enable Unattended Start Mode
  3. Disable Unattended Start Mode
  4. Remove Supervisory Password
  5. Update System Firmware
  6. Display Event / Error Log
  7. View or Set Vital Product Data
  8. Copy Remote Files
  9. Remote Initial Program Load Setup
 10. Manipulate Dead Man Timer
 11. Change Management
 12. Prepare Hard Disk

 Enter    -   Esc=Quit    -   F1=Help    -
-----------  --------------  -------------
```

Figure 6. Utilities Selection Panel

2. Make your selection. Additional panels appear to prompt you for additional information, and messages appear to indicate that the task is completed.

Setting the Supervisory Password

If a password is set and the server is configured to come up in unattended mode, you must enter the password before you can access the firmware System Management Services. The MSS Server is initially shipped with a password of **mss**. This utility allows you to set and change the password.

Note: You can perform this function only if you do it immediately after you perform a power-on reset.

1. Select **Set Supervisory Password** from the utilities panel.

   The *Set Supervisory Password* panel appears (Figure 7 on page 34).

2. Type your new password and press **Enter**. The system prompts you to enter your new password again.

   Note: The supervisory password can consist of from 1 to 8 characters with no restrictions on which characters can be used.

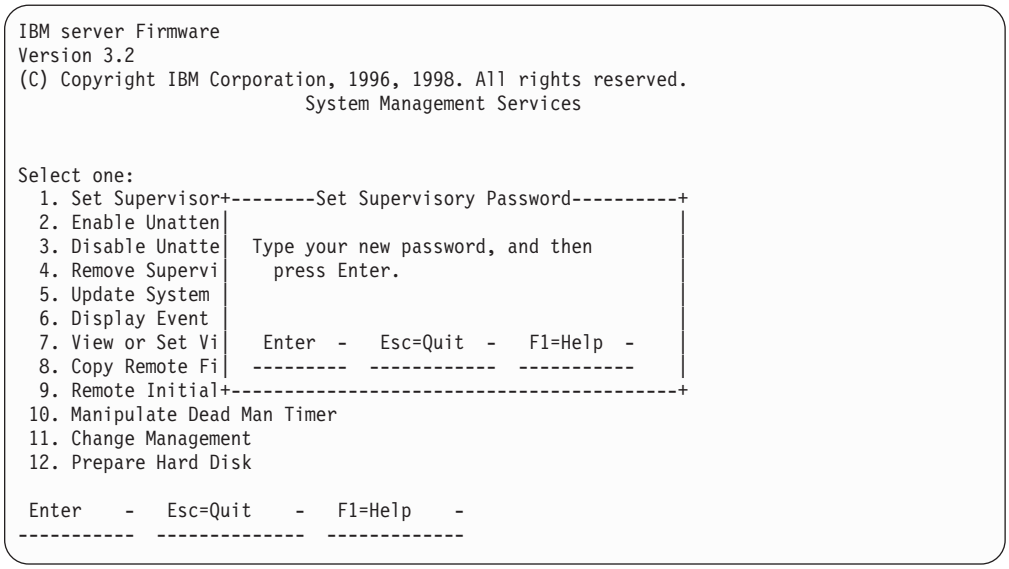


Figure 7. Set Supervisory Password Panel

3. Type the password again and press **Enter**.
4. The *Password Saved* panel appears with the message that your supervisory password has been saved.

Enabling Unattended Start Mode

The default is that the unattended start mode is enabled, which causes the MSS Server to load operational code automatically.

Note: You can perform this function only if you do it immediately after you perform a power-on reset.

1. Select **Enable Unattended Start Mode** from the utilities panel.

   The *Unattended Start Mode Changed* panel appears. See Figure 8 on page 35.

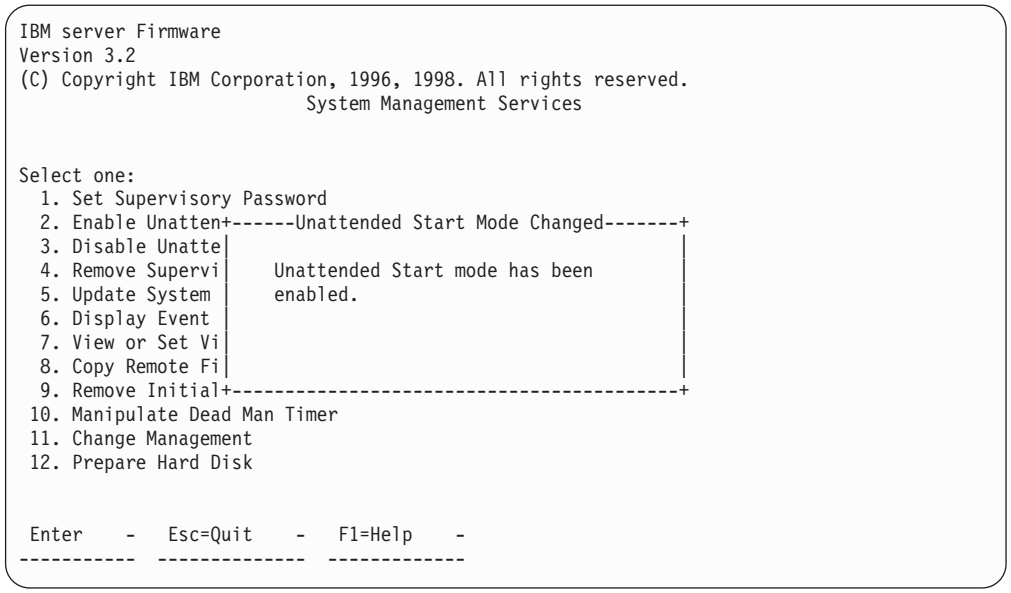


Figure 8. Unattended Start Mode Changed (Enabled) Panel

Note: Once unattended start mode has been enabled, you can enter the firmware by pressing and holding **Ctrl-C** or pressing **F1** at the terminal keyboard when the boot process begins.

Disabling Unattended Start Mode

The default for the MSS Server firmware is that the unattended start mode is enabled. You disable Unattended Start Mode using this utility.

Note: You can perform this function only if you do it immediately after you perform a power-on reset.

1. Select **Disable Unattended Start Mode** from the utilities panel.

   The *Unattended Start Mode Changed* panel appears. See Figure 9 on page 36.

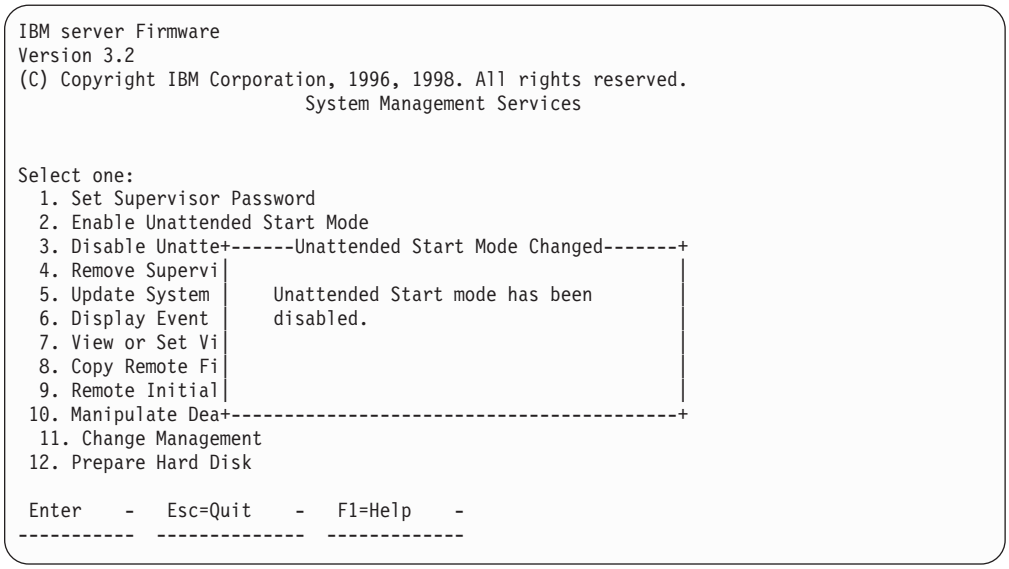


Figure 9. Unattended Start Mode Changed (Disabled) Panel

Removing Supervisory Password

The use of a supervisory password allows you a degree of security by preventing unauthorized access to the MSS Server's System Management Services (firmware). Removing the enforcement of a password, however, could be a convenience while servicing the MSS Server.

Note: You can perform this function only if you do it immediately after you perform a power-on reset.

1. Select **Remove Supervisory Password** from the utilities panel.

   The *Remove Supervisory Password* panel appears. See Figure 10.

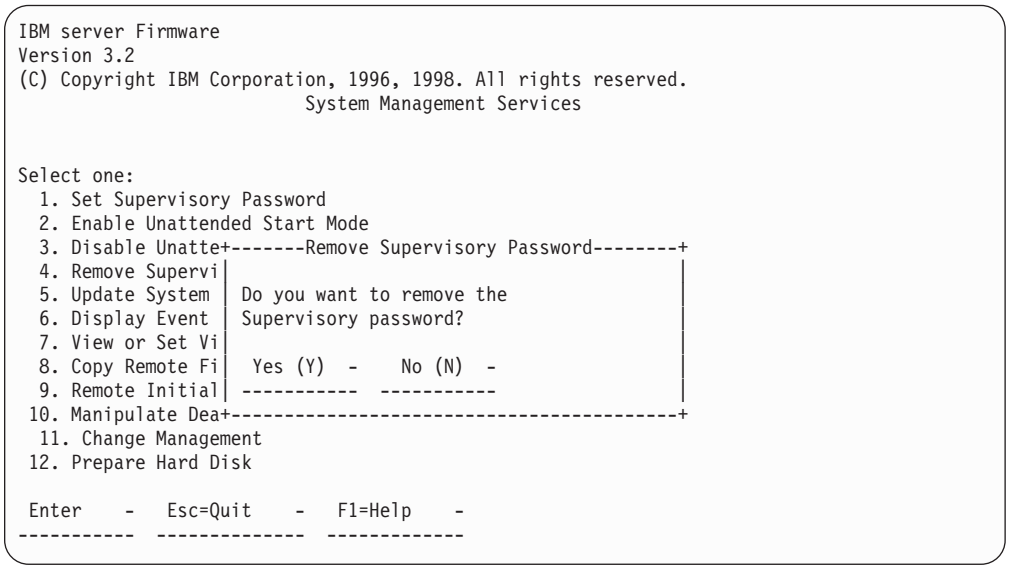


Figure 10. Remove Supervisory Password Panel

2. Type **Y** if you want to remove the supervisory password.
3. The *Password Removed* panel appears. This panel informs you that the supervisory password has been removed.

Updating System Firmware

Use this utility to update the MSS Server firmware.

Note: Do not power off or reset the MSS Server during the process of updating the firmware. If the update fails, the MSS Server will boot a backup firmware image. If this happens, repeat the update procedure to reload the onboard firmware image.

1. Select **Update System Firmware** from the utilities panel.

   The *System Firmware Update* panel appears. See Figure 11.

```
IBM server Firmware
Version 3.2
(C) Copyright server Corporation, 1996, 1998. All rights reserved.
                           System Management Services


Select one:
  1. Set Supervisory Password
  2. Enable Unattended Start Mode
  3. Disable Unattended Start Mode
  4. Remove Supervisory Password
  5. Update System +----------F/W Update Options--------------+
  6. Display Event |                                           |
  7. View or Set Vi| 1. TFTP a Remote Image File               |
  8. Copy Remote Fi| 2. XMODEM a Remote Image File             |
  9. Remote Initial| 3. Use a Local Image File                 |
 10. Manipulate Dea|                                           |
 11. Verify Hard Di|  Enter -  Esc=Quit -   F-1=Help           |
 12. Change Managem| -------   ---------    ------------------|
 13. Prepare Hard D+-------------------------------------------+

 Enter    -   Esc=Quit    -   F1=Help    -
-----------  --------------  -------------
```

Figure 11. Update System Firmware Panel

2. Select the option that you want to use from those listed. For TFTP, the system prompts you for the remote (the “from”) file name that you want to use.

   If you need to set the IP address of the MSS Family Client, use the **Remote Initial Program Load** menu.

   The firmware update process begins. It informs you that the system firmware has been updated.

Displaying the Event/Error Log

To display the Event/Error Log:

1. Select **Display Event / Error Log** from the utilities panel.

   The *Event / Error Log* panel appears. See Figure 12 on page 38.

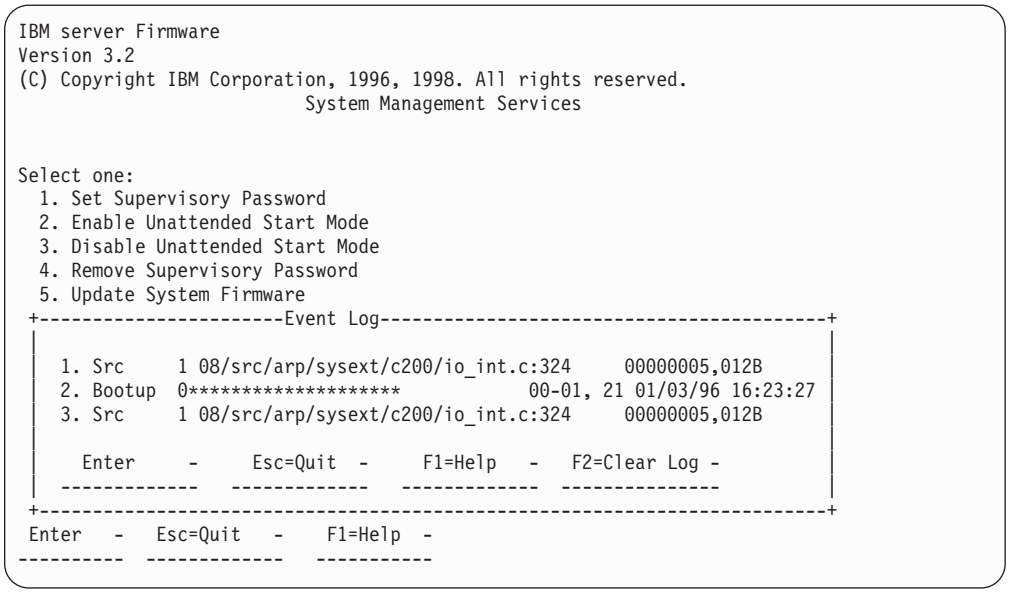


Figure 12. Event/Error Log Panel

If the log is too large to appear on one panel, you can move through the log by using the up and down arrow keys or the PgUp/PgDn keys.

2. Press **F2** to clear the log.

Hardware Error Codes

The error log that is displayed when you use the Display Event/Error Log firmware utility contains error codes. Table 2 explains these codes.

Table 2. Hardware Error Codes

Error Code	Physical Location	Software Subsystem	Explanation
00010000	System Board	Processor	Error occurred during processor test
00011000	System Board	NVRAM	Non-volatile RAM Test Failure
00015001	System Board	Firmware	Error occurred while erasing the system firmware
00015002	System Board	Firmware	Error occurred while updating the system firmware
00015011	System Board	Main Flash Array	Error occurred while erasing the system main flash array
00015500	System Board	Interrupts	System board interrupt test failure
00015501	System Board	Interrupts	Error occurred during processor interrupt test
00015502	System Board	Interrupts	Error occurred during real-time clock interrupt test
00015503	System Board	Interrupts	Error occurred during timer interrupt test
00015504	System Board	Interrupts	Error occurred during dead-man timer interrupt test
00016000	System Board	RTC-NVRAM	CRC error
00016002	System Board	RTC-NVRAM	Read/write failure

Table 2. Hardware Error Codes (continued)

Error Code	Physical Location	Software Subsystem	Explanation
00017001	System Board	RTC-NVRAM	Battery drained
00017006	System Board	RTC-NVRAM	Security data missing or not valid
00017007	System Board	Security	Maximum unsuccessful attempts to enter password was reached
00170000	IDE	IDE	Unable to allocate memory for IDE diagnostics
001701xy	IDE	IDE	IDE device id y on controller x is not responding
001702xy	IDE	IDE	Formatter device error occurred on IDE device ID y on controller x
001703xy	IDE	IDE	Sector buffer error occurred on IDE device ID y on controller x
001704xy	IDE	IDE	Controlling microprocessor error occurred on IDE device ID y on controller x
001706xy	IDE	IDE	Two masters may not be present on IDE controller x. This configuration is not valid.
001707xy	IDE	IDE	IDE device id y on controller x not is responding
001708xy	IDE	IDE	IDE device id y on controller x not is responding
2209E000	System Board	Thermal Sensor	Thermal sensor configuration error occurred
2259E000	System Board	Thermal Sensor	Thermal sensor interrupt error occurred
2269Exxx	System Board	Thermal Sensor	Thermal sensor reached maximum operating conditions. xxx=temperature over maximum conditions in degrees Celsius in hexadecimal
30001000	IDE	IDE	Error occurred while running the IDE diagnostics
30002000	IDE	IDE	Error occurred while preparing the hard drive
5abcdefg	System Board	PCMCIA	Error occurred during the PCMCIA test abcdefg = detailed information
50001100	System Board	Firmware	The level of System Management Services does not match the level of system firmware
710sdddd	155-Mbps MMF adapter	ATM diagnostics	Error occurred with ATM adapter in slot “s” dddd = detailed status
720sdddd	155-Mbps SMF adapter	ATM diagnostics	Error occurred with ATM adapter in slot “s” dddd = detailed status
740sdddd	8260 ATM interface	ATM diagnostics	Error with the 8260 ATM interface dddd = detailed status
750sdddd	FDDI Adapter	FDDI diagnostics	Error occurred with FDDI adapter in slot “s” dddd = detailed status

Table 2. Hardware Error Codes (continued)

Error Code	Physical Location	Software Subsystem	Explanation
7msceddd	PCI slots		Adapters m=unique for adapter type s=subtest, c=slot id, e=error id, ddd = debug
80000000	System Board	8260 Interface	Echo Response test with 8260 failed
801000xy	System Board	Mailbox Memory	Error mailbox memory x = indicates page 2 error y = indicates page 1 error
81xyzzzz	System Board	Memory	Error occurred while testing main flash array memory pages x, y, zzzz = detailed information

Viewing Vital Product Data

This utility allows you to view vital product data (VPD) for the MSS Server

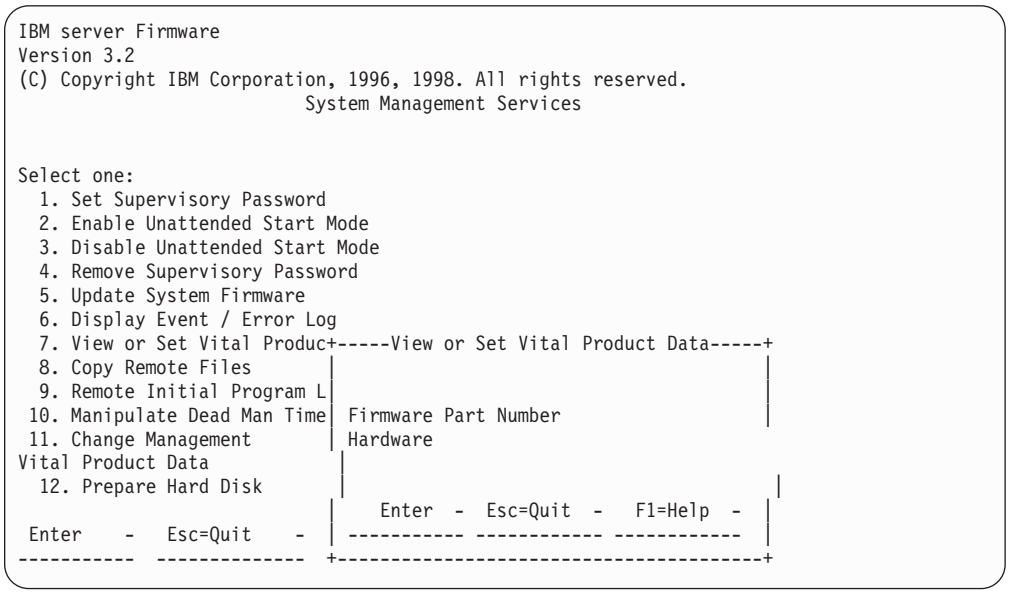


Figure 13. View of Set Vital Product Data

1. Select **View or Set Vital Product Data** from the utilities panel.

   The *View or Set Vital Product Data* panel appears (Figure 13). From this panel you can select the type of vital product data you want to view.

2. For each selection, a *View Part Number* panel appears that contains the part number you selected. Version number and dates are provided for the firmware and System Management Services.
3. Select **Hardware Vital Product Data** if you want to view vital product data. VPD is stored in keyword format. The following is a list of the keywords and their meanings. Depending on the configuration of your system, all of the keywords listed may not be present or have meaningful values.

   Vital product data fields are:

   AT - Main logic card type

DS - Text description of card
FN - FRU number
PN - Manufacturing part number
ML - Maintenance level
MF - Manufacturing location
SN - Serial number
BF - Boot flash level and ID
NA - Burned in MAC Address in ASCII Format
ZB - Burned in MAC Address in Hex Canonical Format
TM - Machine type and model
F# - Feature Number
BS - Box serial number
RC - Recycle count
Z0 - Vendor ID

4. Press **Esc** when you are through.

Copying Remote Files

This utility allows you to copy remote files from another machine into the hard file. There are two methods of file transfer, TFTP from a server using the Ethernet port, or Xmodem over the active serial port.

1. Select **Copy Remote Files** from the utilities panel.

   The *Copy Remote Files* panel appears (Figure 14). From this panel you select the method of file transfer. Subsequent panels allow you to enter the names of the files that you want to copy.

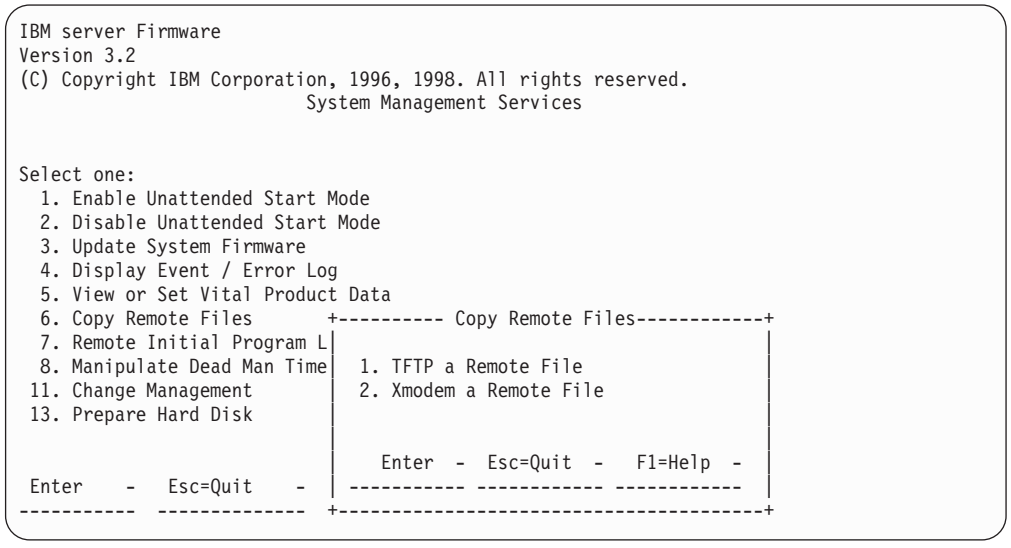


Figure 14. Copy Remote Files Panel

Setting Up Remote Initial Program Load

Before you can configure an MSS Server in the network, it must have an IP address that is recognized within your network and it must have the addresses of your ATM adapters.

This utility allows you to load this minimum information to install this device in your network so that you can send it a configuration file, or otherwise communicate with it. This utility allows you to Ping the MSS Server, after loading its minimum network parameters, to see if you can communicate with it.

1. Select **Remote Initial Program Load Setup** from the utilities panel.

   The *Network Parameters* panel appears (Figure 15). From this panel you can select to enter the IP address of the MSS Server and the host, input adapter parameters, or Ping from the MSS Server to the host.

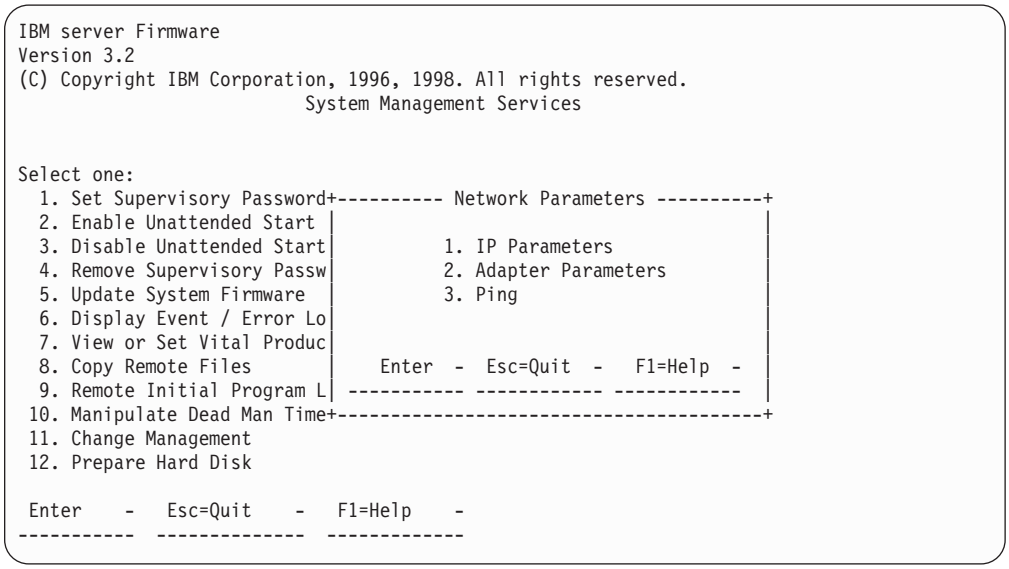


Figure 15. Setup Remote Initial Program Load Panel

- If you select **IP Parameters**, a panel appears on which you can enter:
  - Client IP Address (the IP address of the MSS Server)
  - Server IP Address
  - Gateway IP Address
  - Subnet Mask

  An MSS Server 8210-001 2-wide blade comes from the factory with the following default IP addresses:

  Client 10.1.1.2

  Server 10.1.1.1

  Gateway 10.1.1.1

  Subnet Mask 255.255.255.0

  An A-MSS Server Module 1-wide blade comes from the factory with the following default IP addresses:

  Client 10.1.2.2

Server
10.1.2.3

Gateway
10.1.2.3

Subnet Mask
255.255.255.0

2. If you select **Adapter Parameters**, a panel appears with a list of any configurable adapters.
3. The **Ping** option allows you to test connectivity.

   Note: Do not Ping your current terminal connection via SLIP.

Manipulating the Dead Man Timer

This utility allows you to selectively enable or disable the dead man timer. The default is disabled.

1. Select **Manipulate Dead Man Timer** from the utilities panel.

   A *Dead Man Timer Options* panel appears. From this panel you can enable or disable the timer.

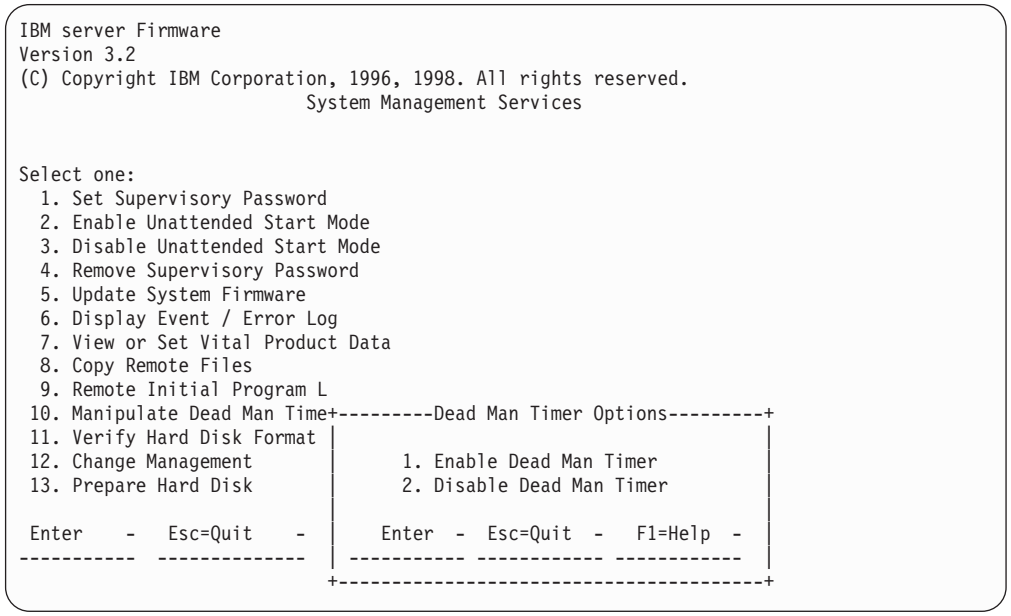


Figure 16. Manipulate Dead Man Timer Panel

If you have enabled the timer and the server locks up, the timer automatically resets the hardware after the time expires.

Change Management

Change Management enables you to manipulate the server level of software code that will run on the server See “Chapter 9. Using BOOT Config to Perform Change Management” on page 113 for detailed information about change management.

Xmodem Software Selection

Xmodem is supported only from the Firmware prompt. To access the Firmware prompt, you must either interrupt the boot-up sequence or bring up the server in attended mode. The Change Management command is available from the Utilities option of the Main Menu. From that point, the server directs you as to what to transfer in and where to put the image.

Notes:

1. When the server is in firmware mode, there is no Active configuration or image. Therefore, you should use caution when specifying where to write new images or configurations.
2. When using Xmodem to transfer a multiple load module image (in the form of several files ending in .ld), ***you must*** transfer each of the modules (.ld files) one by one to get the entire load module image.

   When an entire load image has transferred, the status of the bank will change from CORRUPT to AVAIL. Transfer file LML.ld first. Unless you see an information message `ERROR WRITING FILE` appear, assume each individual transfer has been successful.

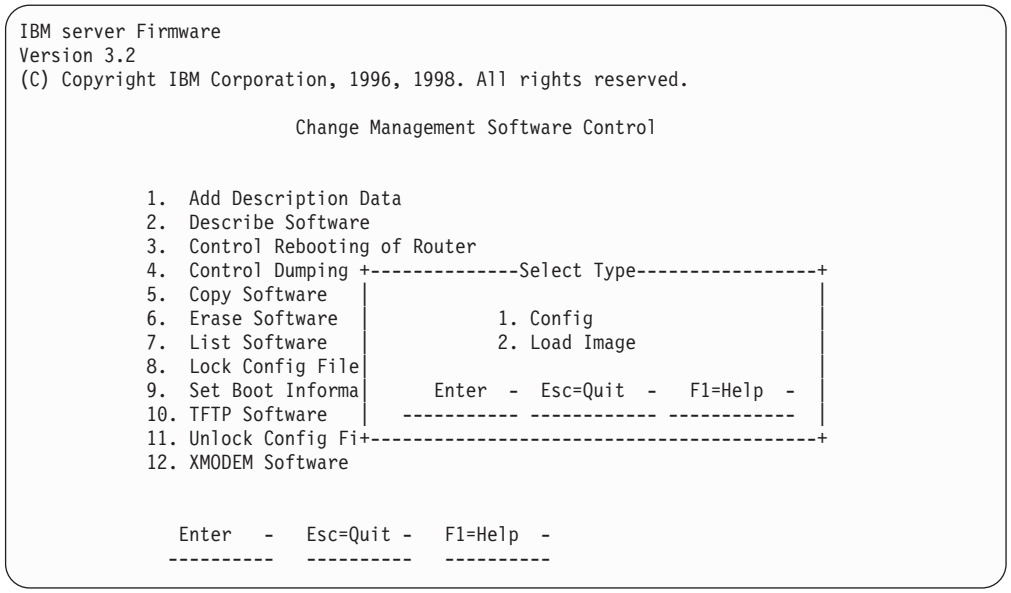
When you are finished with file transfer, select **List software** on the Change Management menu. The status will have changed to AVAIL for that bank that has the new load image.

The following sample menus are associated with Xmodem download. These menus show the text that is displayed when you choose Change Management.

Examples:

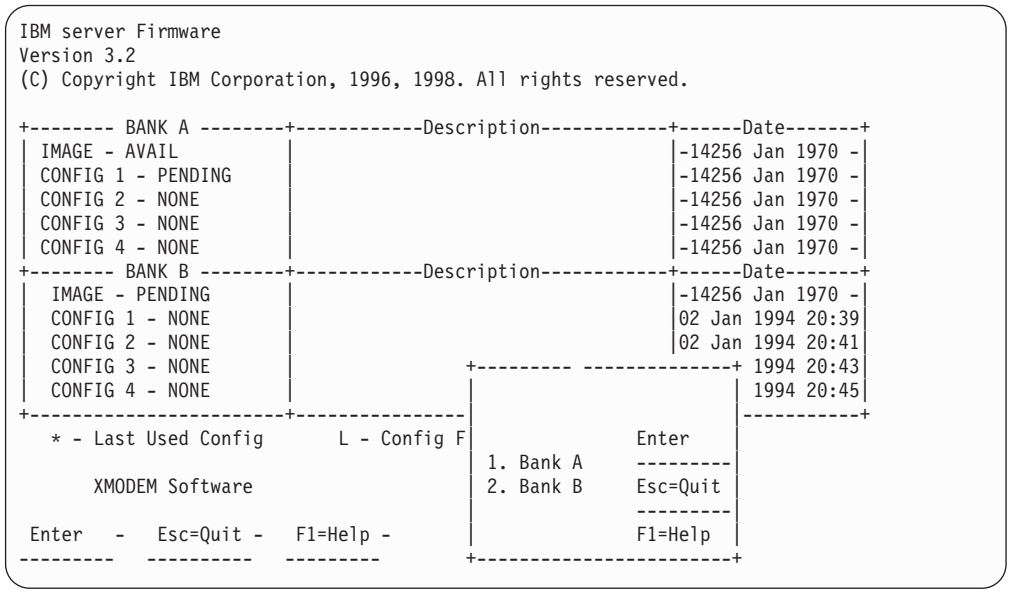
```
IBM server Firmware
Version 3.2
(C) Copyright IBM Corporation, 1996, 1998. All rights reserved.

                          Change Management Software Control

            Select one:
            1.  Add Description Data
            2.  Describe Software
            3.  Control Rebooting of Router
            4.  Control Dumping of Router
            5.  Copy Software
            6.  Erase Software
            7.  List Software
            8.  Lock Config File
            9.  Set Boot Information
            10. TFTP Software
            11. Unlock Config File
            12. XMODEM Software


            Enter   -   Esc=Quit -   F1=Help  -
           ----------   ----------   ----------
```

1. Select **Copy Software**.

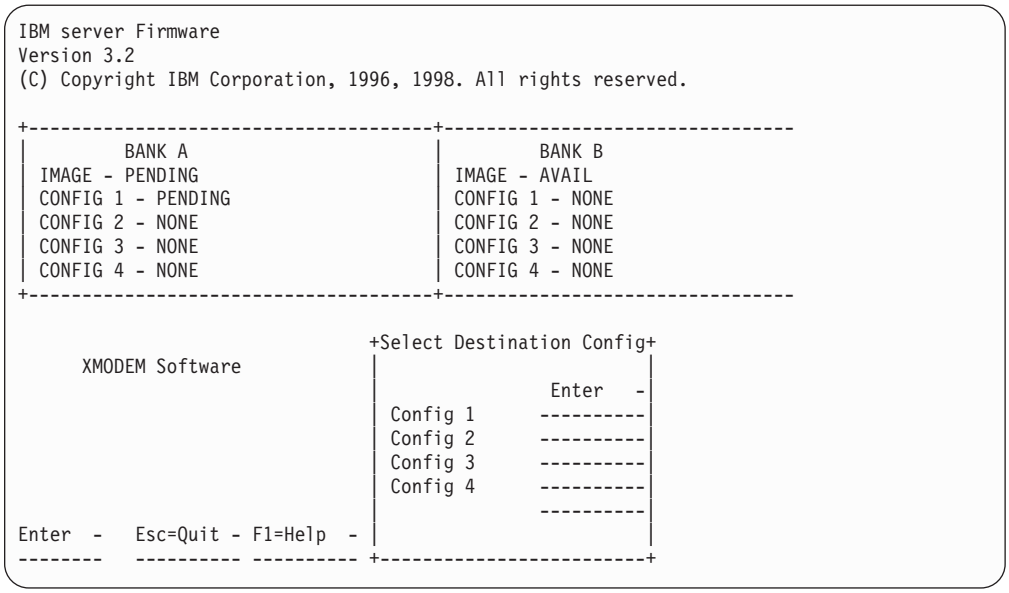


2. Select either **Config** (for configuration file) or **Load Image** (for the operational software file).

The following figure is an example of the Load Image selection.



The following figure is an example of the Config selection.


IBM server Firmware
Version 3.2
(C) Copyright IBM Corporation, 1996, 1998. All rights reserved.
BANK A
IMAGE - PENDING
CONFIG 1 - PENDING
CONFIG 2 - NONE
CONFIG 3 - NONE
CONFIG 4 - NONE
BANK B
IMAGE - AVAIL
CONFIG 1 - NONE
CONFIG 2 - NONE
CONFIG 3 - NONE
CONFIG 4 - NONE
XMODEM Software
Select Destination Config
Enter
Config 1
Config 2
Config 3
Config 4
Enter - Esc=Quit - F1=Help -

Chapter 4. Getting Started with Configuring the 8210

This chapter explains how to access the 8210 using a workstation and how to manage operational software images and configuration files. It also provides a brief overview of the configuration methods available for the 8210.

Physical Access Methods

Before the 8210 has been configured, it cannot yet function in the ATM network. Therefore, you have to access it in one of the following ways:

- Through a null modem cable attached to the EIA 232 service port. This is known as local connection.
- Through one of the PCMCIA modems, or through a modem attached to the EIA 232 service port. The PCMCIA modems are the Voice/Data/Fax Modem and the Data/Fax Modem. These are the forms of remote connection, which rely on the telephone lines.

You can set up both a local and a remote connection to the 8210. However, only one port can be active at any given time. If a workstation is connected locally to the serial port and a call comes in over the Voice/Data/Fax Modem or the Data/Fax Modem, priority is given to the call. After the call, the workstation will have to log back into the 8210.

With local or remote connection, you can use a teletypewriter (TTY) connection. TTY requires communications software to enable file transfer.

Alternatively, you can use Serial Line Internet Protocol (SLIP) over the local or remote connection. If you use SLIP, you must have Transmission Control Protocol/Internet Protocol (TCP/IP) running on your workstation.

You can continue to use local or remote access to the 8210 after it has been configured. However, after configuration, you can also use Internet Protocol (IP) to access the 8210 through the network. For the IBM 8210 Nways Multiprotocol Switched Services (MSS) Server, the connection is made over optical fiber from one of the ATM connectors. For the IBM Nways Multiprotocol Switched Services (MSS) Server Module, the connection is made through the ATM switch in which the module is installed.

Figures 17, 18, and 19 show local connection, remote connection using the PCMCIA modem, and connection over the network.

© Copyright IBM Corp. 1996, 1998

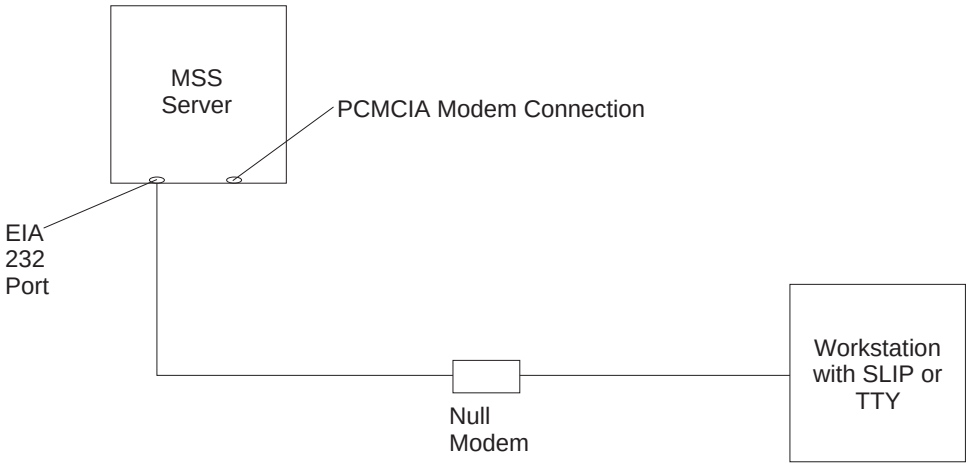


Figure 17. Local Serial Connection to the EIA 232 Port

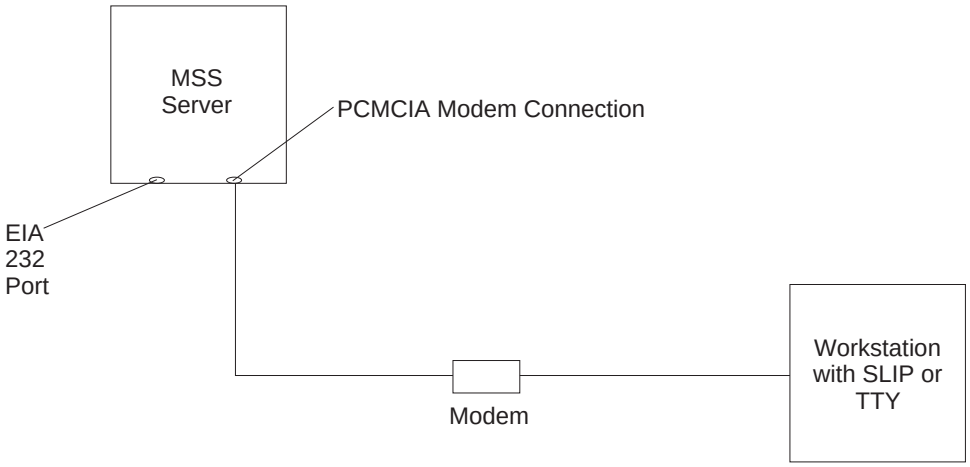


Figure 18. Remote Serial Connection to the PCMCIA Modem (Voice/Data/Fax Modem or Data/Fax Modem)

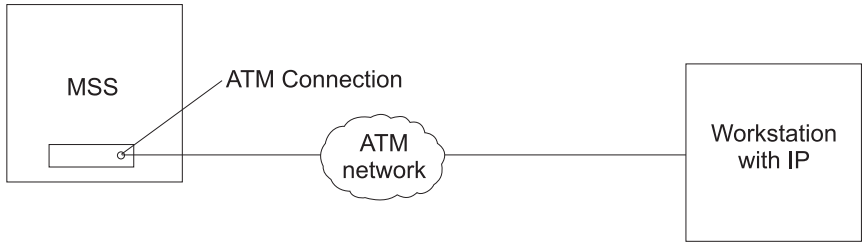


Figure 19. Connection Using IP Over the ATM Network. The server must be operational in the network to use this connection.

SLIP Addresses

To configure SLIP, use these addresses:

The IP address of the workstation
10.1.1.3

The IP address of the 8210
10.1.1.2

For instructions about installing SLIP on your workstation, refer to the documentation for your version of TCP/IP.

Serial Port and Data/Fax Modem Default Settings

These are the default settings for the serial port:

Speed 19.2 Kbps

Parity None

Data Bits
8

Stop Bits
1

The Data/Fax Modem is a 28.8-Kbps V.32 bis modem. It is set up with a default speed of auto detect. The parity, data bits, and stop bits are the same as those of the serial port: None, 8, and 1.

Once the operational code has loaded, the line speed for the serial port is automatically set to 19200 baud.

Configuration and Monitoring Tools

These are the various configuration and monitoring tools that are supported by the physical connections:

Multiprotocol Switched Services Client Configuration Program
This is a standalone program that is installed in a workstation which uses TCP/IP to connect to the 8210. You must use this program differently before and after the initial configuration of the 8210.

Before configuration:

Initial configuration of the 8210 must be through a modem or the service port, over a serial link. When the 8210 is in this state, you cannot use the Communications options of the Configuration Program. You can create configuration files and download them later to the 8210 over the serial link using TFTP over SLIP. The workstation must be running TCP/IP with a TFTP daemon.

Note: If you are using a Windows 95 workstation, you must obtain a TFTP daemon as the daemon is not part of the base TCP/IP software.

After configuration:

The configuration file that download over a serial link can provide an IP address and subnet mask to the 8210, or establish LAN emulation. After configuring the 8210 and making it operational in the ATM network, you can access the 8210 through the network.

When the 8210 is in this state, you can use the Communications Send option of the Configuration Program to send configuration files from the

workstation over the network to the 8210. When using the version of the Configuration Program that is supported by AIX, you can also use the Communications Retrieve option of the Configuration Program to retrieve configuration files from the 8210. For more information, see *User's Guide for Nways Multiprotocol and Access Services Products*, GC30-3830.

Web browser Hypertext Markup Language (HTML) interface

The Web browser interface is a configurator that is a home page and is accessed by a Web browser from a workstation that is connected to the 8210. You need a Web browser that can display clickable images and tables. The Web browser interface can be accessed using SLIP or IP. You must use the serial line connection and SLIP before the 8210 is operational in the network.

If you supply the Web browser the SLIP address, one of the configured IP addresses of the 8210, or its name (when using an IP name server), the Web browser interface will come up.

Note: The configured IP addresses of the 8210 include the IP addresses of all the LAN emulation clients and Classical IP clients.

Command line interface

The command line interface is a teletypewriter (TTY) text interface that requires you to enter commands to use it. The workstation that accesses it must be either an ASCII terminal, a personal computer (PC), or other intelligent programmable workstation emulating an ASCII terminal.

This interface must be reached over a serial link before the 8210 is operational in the network; you can use TTY or SLIP to access it. If you use SLIP, you can Telnet into the 8210.

After the 8210 is operational in the network, you can Telnet into the 8210 over IP to bring up this interface. If one connection to the 8210 is a Telnet session, the 8210 can support two connections at one time.

The command line interface is marked by an asterisk (*) prompt.Refer to the *IBM Multiprotocol Switched Services (MSS) Server Interface Configuration and Software User's Guide* for a full description of this interface.

Important: If you use a serial connection, (either local or remote), you ***must press a key*** to bring up the asterisk that is the prompt for the command line interface. When you make the connection, the message `Please press a key to obtain console` appears and reminds you to do this.

Voice/Data/Fax Modem or Data/Fax Modem

The Voice/Data/Fax Modem is an integrated modem with both voice and fax capabilities that is shipped with the 8210 in the U.S. and Canada. It provides access using touch tone telephone input with automated voice responses. In addition to faxing an alert after the 8210 has had a failure and has restarted, it can fax other reports that monitor the 8210 and it can change a few dynamic parameters that help to maintain the 8210 in the network.

The Data/Fax Modem is an integrated PCMCIA modem that handles data and can fax an alert from the 8210. For example, it can fax an alert from the 8210 if the 8210 has had a failure and has then automatically restarted.

Both of these modems provide full text console access to the command line interface. They provide remote connection that supports either the TTY or SLIP access. The Voice/Data/Fax Modem provides access using the voice interface to several configuration parameters, including enabling or disabling thermal shutdown for the standalone server only.

Fax Accumulation

If several undeliverable faxes are sent from the Voice/Data/Fax interface, they will not be deleted. They will accumulate as new faxes are added and sent when possible. The most common cause of fax delivery failure is a missing or incorrect fax telephone number.

Local and Remote Console Access

When accessing the 8210 locally on a null modem cable attached to the EIA service port or remotely through the PCMCIA modem, use VT100 terminal emulation. Because VT100 does not define function keys above F4, edit the keyboard mapping manually as follows: For F6, enter the mapping (ESC)OU. For F9, enter the mapping (ESC)(Left square bracket)009q.

Note: (ESC) represents the carat symbol followed by the left square bracket.

Also note that a PING done on the PCMCIA modem may take up to 2 minutes.

Remote Voice Access

When dialing the number for voice access to the MSS Server, detection of the user is not automatic, as implied in “Voice/Data/Fax Modem Menu Items” on page 70. The user will be asked to press the # key. If the user fails to do this, the server assumes the caller is a modem and will subsequently send a carrier signal. If the # key is pressed, operation proceeds as given in “Voice/Data/Fax Modem Menu Items” on page 70.

File Transfer

Table 3 defines the ways in which configuration files and operational software files can be transferred to and from the 8210.

Table 3. File Transfer

File Transfer Method	Type of Connection
TFTP Get command from the 8210 to the workstation that has the binary configuration file, to download operational software images and configuration files to the 8210. Files sent using TFTP must be binary, or the 8210 cannot use them. You should use the Create command of the Configuration Program to save configuration files in binary format before downloading them to the 8210. After the 8210 is operational in the network, you can use the TFTP Put command over IP to upload a file from the 8210 to a workstation. The file will be uploaded in binary format. Both operational software and configuration files can be uploaded. You should use the Read router configuration option of the Configuration Program to make an uploaded configuration file usable by the Configuration Program so that you can change some parameter values in it. **Note:** Using TFTP Put is a way to retrieve files from the 8210 if the Retrieve option of the Configuration Program is not available.	• SLIP connection (using the TFTP Get command to download files to the 8210). • IP connection of operational 8210 over functioning network (using the TFTP Get and Put commands to download and upload files).
The Communications Option of the Configuration Program (actually, the protocol for this is SNMP). This method cannot be used until the 8210 is operational in the network. The files are not binary, but are in a format that is internal to the Configuration Program. This function can send configuration files to the 8210 and retrieve them from the server.	IP connection of operational 8210 over functioning network.

Initial Configuration

After the 8210 has passed its hardware diagnostics, it is in a ready state for configuration. These are two examples of ways to complete the first configuration:

First Example

1. Use the Configuration Program to create a binary configuration file.
2. Download the file to the 8210 using TFTP over SLIP.
3. Restart the 8210 to make the configuration active. If your configuration file included all the necessary parameters, the 8210 should now be completely operational in the network.

Second Example

1. Perform a minmial configuration using one of the following methods:
   - Use a SLIP or a TTY connection over a serial link to access the IBM 8210.
   - Bring up the Web browser interface or the command line interface.
   - Use quick configuration to do a minimal configuration of the IBM 8210, including IP address and SNMP. See “Quick Configuration” on page 53.
2. Restart the IBM 8210 to activate the quick configuration.

3. Next, make and save a configuration file using the Configuration Program. Use either the TFTP Get command over SLIP or IP or use the Communications Options Send command of the Configuration Program to download the configuration file.

   When using TFTP, you must use the Create option of the Configuration Program to create binary files and then TFTP them to the IBM 8210.
4. Restart the IBM 8210 to make the configuration active. If the configuration file included all the necessary parameters, the IBM 8210 should now be completely operational in the network.

Tips for Managing Configuration Problems

Important: After the IBM 8210 is configured and operational, ***always*** back up the active configuration file. Keeping this file enables you to re-establish the IBM 8210 on the network should the active configuration become corrupted.

Back up the active configuration file by retrieving it and storing it in the workstation. See “File Transfer” on page 52 for more information.

Reconfiguring

You may find it hard to detect problems caused by configuration errors. A configuration error can initially appear to be a hardware problem because the IBM 8210 will not start or data will not flow through a port. In addition, problems with configuration may not result in an error initially; an error may occur only when specific conditions are encountered or when heavy network traffic occurs.

If you cannot resolve a problem after making a few changes to the configuration or after restoring the active configuration file, it is recommended that you generate a new configuration. Too many changes to a configuration often compound the problem, whereas you can usually generate and test a new configuration within a few hours.

Quick Configuration

Quick configuration is a process for initial configuration that is available either from the Web browser interface or from the command line interface. It produces a simple configuration that will enable the IBM 8210 to run in the network. The Web browser interface, which is the more usable of the two interfaces, is recommended. See “Quick Configuration Using the Web Browser Interface” on page 63 for a description of quick configuration using the Web interface.

Completing the Configuration After Quick Configuration

After completing quick configuration, reload the IBM 8210 to activate the configuration. Then, you can access the IBM 8210 over the network, if you have configured an IP address for it.

The configuration provided by QCONFIG depends upon many default values for parameters, some of which may not be appropriate to your installation. You may need to modify the configuration created using QCONFIG to customize the IBM 8210 to work in your network. Do this using any of these methods:

- Configuration Program
- Web browser HTML interface
- Command line interface

However, the Configuration Program is the preferred configuration method for these reasons:

1. It enables you to keep a number of copies of configuration files on a server for uploading to the appropriate IBM 8210s.
2. It does not alter any configuration parameters dynamically. This feature helps control changes to the IBM 8210 configurations.
3. It performs more input validation and cross-checking of the configuration parameters than the other methods.

The command line interface and the Web browser interface cause certain parameters to be altered dynamically. The binary files that they create are saved on the hard disk ofthe IBM 8210, not in the workstation. These characteristics make them more difficult to use for managing the configuration of the IBM 8210. However, they can be used to monitor the operations of the IBM 8210, whereas the Configuration Program cannot. They are also useful when you want to change one of the parameters that can be dynamically altered.

How Software Files Are Managed

To help manage operational software upgrades and configurations, the IBM 8210 has a software change management feature. This utility enables you to determine which operational software file and which configuration file is active while the IBM 8210 is running. In addition to storing the active operational software and the active configuration file, the IBM 8210 stores two backup images of the operational software and up to 11 configuration files in non-volatile memory.

How to View the Files

To use the change management tool in the command line interface to view the operational software image and the configuration files, follow these steps:

1. From the prompt for OPCON, which is an asterisk (*), type **talk 6**. The prompt `Config>` appears.
2. Enter **boot**. You will see the prompt `Boot config>`.
3. Enter **list** to display information about which load images and configuration files are available and active.

   See “List” on page 121 for sample list output and a description of file statuses.

How to Reset the IBM 8210

Note: A reset interrupts the function of the IBM 8210 for up to 90 seconds. Be sure that the network is prepared for the interruption.

As previously stated, PENDING and LOCAL files are not loaded into active memory until you reset the IBM 8210.

You can reset the IBM 8210 using any one of these methods:

- Press the hardware reset button.
- At the `Config only>` prompt, type **reload**.

Note: The `Config only>` prompt appears when no configuration file is active. Lack of an active configuration file indicates that an active configuration has become corrupted or that the IBM 8210 is not configured.

- At the OPCON prompt (*), type **reload**.

File Transfer Using TFTP

See “TFTP” on page 123 for a sequence of commands to transfer a file from a workstation or server to the IBM 8210 using TFTP. You will need to substitute your own values for the IP address and path, which are given as examples.

Storing Configuration Files Using the Command Line Interface or the Web Browser Interface

To store a configuration file created using the command line interface, type **write** at the `Config>` prompt. When using the Web browser interface, select **Write**. The Write command creates a binary configuration file that contains the most current value of each of the configuration parameters.

This file is stored in the ACTIVE bank and is given PENDING status. If the status of the file is not changed by a Set command, it becomes the ACTIVE configuration when the IBM 8210 is reset.

Changing the Statuses of Files

These are the ways to change the statuses of image and configuration files:

- You can cause the IBM 8210 to perform a reset by using the Send command from the Communications Option of the Configuration Program. When you do this, the file sent can arrive as a PENDING file or as an AVAIL file. If it is a PENDING file, it becomes the ACTIVE configuration and the previously ACTIVE file becomes AVAIL when the IBM 8210 is reset.

  If it is an AVAIL file, resetting the IBM 8210 does not change its status.
- Use the Set config (set config) commands from the `Boot config>` prompt manually to change the status of any files except the ACTIVE files. If you set a file to PENDING, it becomes ACTIVE and the ACTIVE file becomes AVAIL when a reset is performed.
- Use the Write command to store a configuration file that you have created using the command line interface or the Web browser interface, it is stored with a PENDING status.
- If you copy a file from one location to another, the file receives the status of the file that was there before it and that it overwrites. For example, copying a file with the status of AVAIL over a file that has the status of PENDING, the new file will keep the status of the original file, which is PENDING.

Using the Configuration Program to Manage the Configuration Files

For optimal configuration management, it is recommended that you use the Configuration Program and its configuration database to manage all IBM 8210 configuration files.

The design of change management facilitates good control of the configuration files. Keeping the ACTIVE file and the file that is stored in the configuration database the same assures that a copy of the ACTIVE file is always available.

Use the Send option to send a new configuration to the IBM 8210, the new configuration is written to the ACTIVE bank and overwrites the file located in the position just below the currently ACTIVE configuration. The new configuration is PENDING if a time is set for a reset. If the configuration file is sent without a specified time for the reset to occur, it gets AVAIL status.

For example, suppose that CONFIG 2 is ACTIVE. The new configuration file is written to CONFIG 3. It has a status of PENDING if a reset time is associated with it; if not, it has a status of AVAIL.

If the file has a status of PENDING, CONFIG 2 becomes AVAIL and CONFIG 3 becomes ACTIVE when a reset occurs. The next file that is sent from the Configuration Program will be placed in CONFIG 4. If a reset time is associated with the file, it will have the PENDING status and will become ACTIVE when the next reset occurs. If another file is then sent, it is placed in CONFIG 1 because the currently ACTIVE file is now in CONFIG 4. This arrangement results in a circular queue.

If the downloaded file has a status of AVAIL, a reset does not change its status. If another file is sent down, it overwrites that file because the ACTIVE file has not changed and the newly downloaded file always occupies the location just behind the ACTIVE file.

Using the Set Commands

See “Set” on page 122 for information about the **set** command.

Other Change Management Functions

These are the other change management commands:

- Describe load images
- Describe config images
- Disable dumping
- Enable dumping
- Erase files

Describe

See “Describe” on page 118 for information about the **Describe** function.

Disable Dumping

The IBM 8210 can be set up to dump the contents of memory to permanent storage in the unlikely event of a complete system failure. If dumping is enabled, using this selection will cause the IBM 8210 *NOT* to dump to disk.

To disable dumping, type **t 6** at the *, press **Enter** and then type **disable dump** or **dis du** at the `Config>` prompt. You will see the message:

```
Config> Automatic memory dump disabled
```

Enable Dumping

This command enables the dumping of memory without intervention from anyone in the event that the IBM 8210 has a catastrophic error. The IBM 8210 will dump

memory onto the hard disk. Once a successful dump has been taken, the IBM 8210 attempts to restart. Depending upon the failure of the IBM 8210, it cannot always restart. In this case, you should restart it manually and call a service person, who will dial into the IBM 8210 to determine the nature and the causes of the failure.

To enable dumping, type **t 6** at the *, press **Enter** and then type **enable dump** or **ena du** at the `Config>` prompt. You will see the message:

```
Config> Automatic memory dump enabled
```

The default state is to have dumping enabled.

Erase Files

See “Erase” on page 119 for information about the **erase** command.

Using the Copy Command

The Copy command moves a file from one location in the storage area to another. This command allows you to change the status as well. The file moved always receives the status of the storage area that it is moved to. For example, suppose that you have this scenario:

- The configuration file in BANK A CONFIG 1 is AVAIL. The configuration file in BANK B CONFIG 1 is PENDING.
- You copy the configuration in BANK A CONFIG 1 to BANK B CONFIG 1.

In this case, the original configuration file in BANK A CONFIG 1 remains unchanged and AVAIL. The configuration that was in BANK B CONFIG 1 is overwritten by a copy of the configuration file that is in BANK A CONFIG 1. This copy retains the status of the file that it overwrote, in this case, PENDING.

See “Copy” on page 116 for additional information about the **copy** command.

Using the Lock Command

The **lock** command prevents the server from overwriting the selected configuration with any other configuration.

See “Lock” on page 121 for additional information about the **lock** command.

Using the Unlock Command

The **unlock** command removes the lock from a configuration allowing the configuration to be updated.

See “Unlock” on page 127 for additional information about the **unlock** command.

Chapter 5. Using the World Wide Web Interface

The MSS Family Client provides a World Wide Web interface to monitor and configure the product. The Web browser interface performs all of the functionality of the command line interface, but in a graphical, more user-friendly manner.

Connecting to the World Wide Web Interface

There are four mechanisms for accessing the Nways MSS Server using the Web interface:

- Locally, over the service port with a workstation that communicates using Serial Line IP (SLIP).
- Remotely, over an external modem connection to the service port. As with the local connection, the workstation must support SLIP.
- Remotely, using the integrated Voice/Data/Fax Modem or the Data/Fax Modem PCMCIA modem. This connection must also support and be running SLIP.
- Through a LAN emulation (LE) client or Classical IP interface running over the ATM adapter. This connection works over an IBM 8210 that has been configured and is operational in the network.

  To use this connection, provide the browser with the IP address of a LE client or Classical IP interface.

Use any web browser that supports HyperText Markup Language (HTML) tables and clickable images. Examples of browsers that support this feature are WebExplorer Version 1.03 or higher, Netscape Navigator Version 1.1N or higher, and Mosaic Version 2.1.1 or higher.

To access the Home Page of the IBM 8210, point your browser to the Universal Resource Locator (URL) `http://<machine>/`, where <machine> is either the name or one of the configured IP addresses of the IBM 8210.

You will be shown the Home Page that is described in the next section.

Note: Before using the Web browser, the IBM 8210 must have been configured with an IP address. This address can either be a network address or a SLIP address. The default SLIP address for the IBM 8210 is:

`10.1.1.2`

Use this source IP address to identify the workstation:

`10.1.1.`*x*

The letter *x* stands for any value.

Rules for Using the Web Interface

When configuring using the Web browser interface, observe the following guidelines:

- Many configuration options require you to enter data on two or more Web pages (or forms). If you fill in and submit the first form in a series, be sure to complete the remaining forms. If you do not fill in and submit all the forms, the configuration parameter could be left in an unknown state.

© Copyright IBM Corp. 1996, 1998

- More than one person should not perform configuration at the same time. They can interfere with one another. For example, one person could delete an interface while the other person is in the middle of configuring a protocol on that interface.
- Disable the caching feature of the browser. If you do not do this, the browser may pull a page out of memory instead of going to the IBM 8210 to get the latest information. The browser will display old data. This problem is more likely to occur when you use the *Back* button on the browser.
- Do not use your web browser's reload, back, or forward navigation buttons when using the Web browser interface. Using these buttons could cause problems during configuration. Instead, use the command history list or any of the navigation buttons on the web pages themselves.

Home Page Structure

Figure 20 shows the IBM 8210 Home Page.

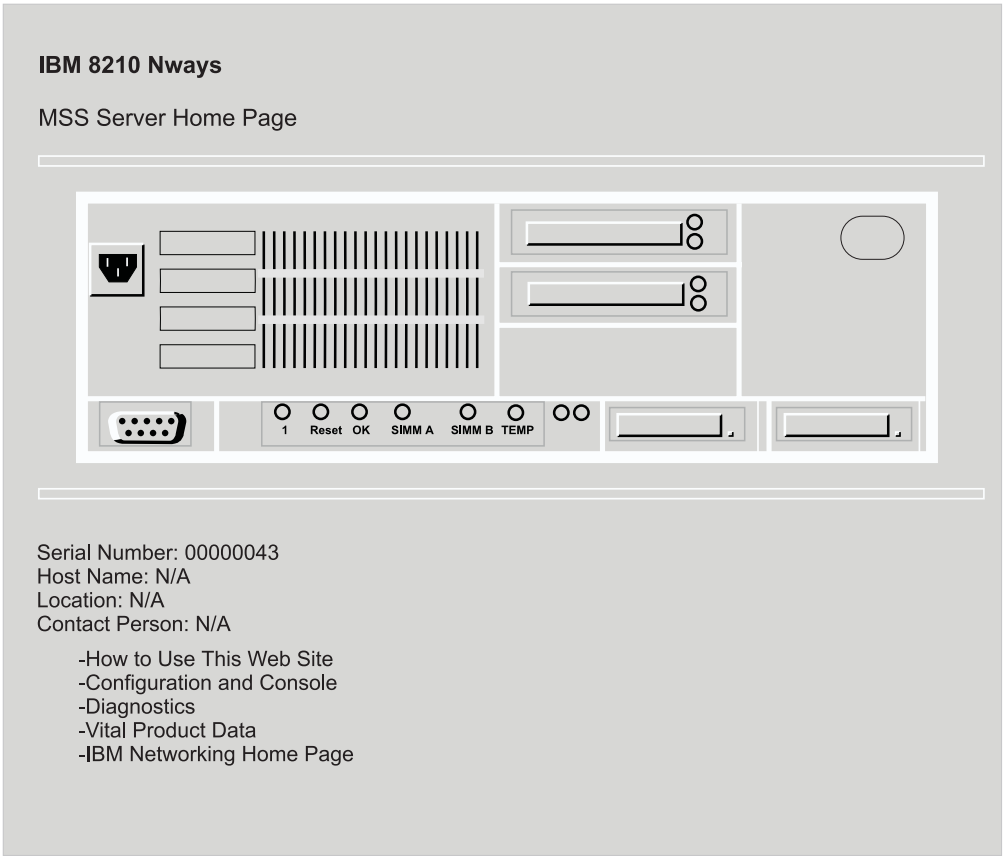


Figure 20. IBM 8210 Home Page

This Home Page provides a graphic that shows the status of the IBM 8210. It indicates the current network interfaces installed and shows the status of each port (for example, installed, enabled, or disabled). The current state of each LED is also shown, as well as the indication of the devices that are installed in the two PCMCIA slots. If the Web browser supports dynamic refresh, then this page will automatically refresh itself approximately every 80 seconds. If you click any of these ports or interfaces, a more detailed description of its status will be shown on a separate Web page.

Click **How to use this Web Site** for instructions about using this site.

Click **Configuration and Console** to bring up the menu shown in Figure Figure 21.

Click **Diagnostics** to bring up the menu shown in Figure Figure 22.

Click **Vital Product Data** for information about the hardware and operational software. This panel, which is usually used for diagnostics, is not displayed here.

Click **Help Server Location Configuration** to set the path for the optional Help Server. You will need to set this path if you want to use the optional help files for the Web Browser interface.

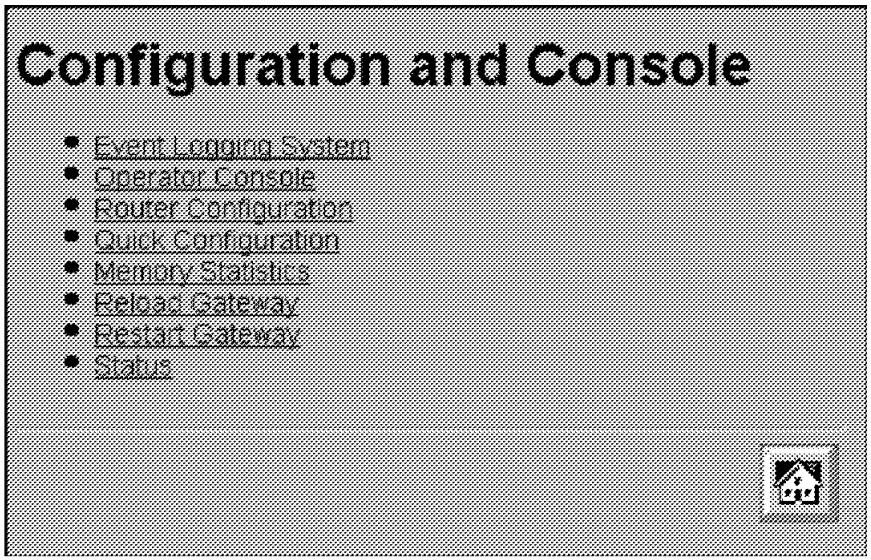


Figure 21. Configuration and Console Page 1

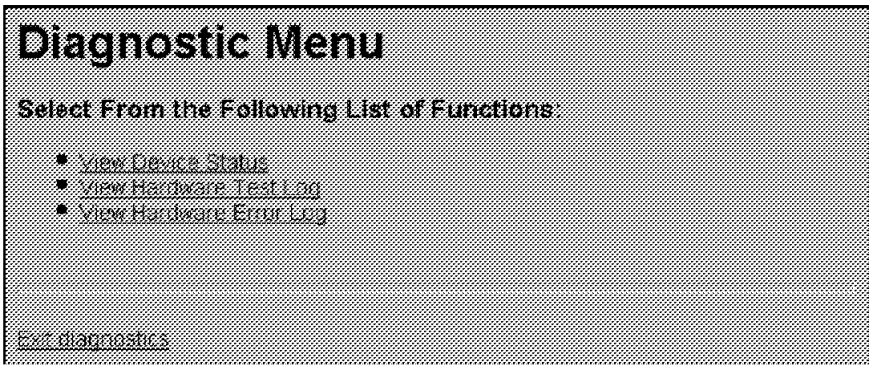


Figure 22. Diagnostic Menu

Configuration and Console Menu

This menu can lead you into various aspects of configuration. To start with quick configuration, click **Quick Configuration**. Figure 23 shows the quick configuration

menu. See “Quick Configuration Using the Web Browser Interface” on page 63 for information about quick configuration and guided configuration.

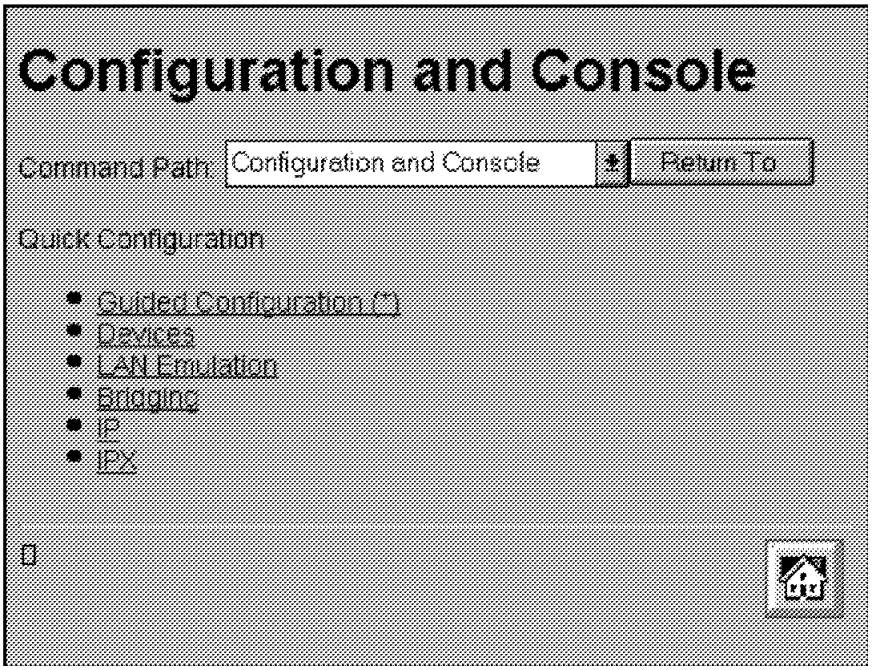


Figure 23. Configuration and Console Page 2

Event Logging System

One of the links on the Configuration and Console page 1 is to the Event Logging System (ELS). The ELS display is similar to the one provided on the command line interface. On the Web interface, going into the ELS will display the most recent events stored in the system memory. In order to get future updates, press the Reload button on your browser. For more details about the ELS message facility, refer to the *Event Logging System Messages Guide*.

Operator Console

The console monitoring interface provides real-time status information very similar to that offered in the command line interface. The menus from the command line interface are presented as a hierarchy of Web links that can easily be traversed with the click of a mouse button. It is possible to jump back several levels in the hierarchy with a single push of a button.

Device Configuration

Important: Exercise caution when using the Web browser to change configuration parameters. Changes to the configuration that are made using the Web browser are written directly to static random access memory (SRAM). You can make unintentional configuration changes that do not take effect until you reset the IBM 8210. To check that you have the correct parameters, look over the settings for any parameters that you have configured before submitting them.

The Web interface greatly simplifies the configuration of network and protocol parameters. In many cases where it is necessary to remember the individual network numbers on the command line interface, those options are now all presented as menu options on the Web. Also, the Web interface uses the graphical features available to it, such as pick lists, selection lists, radio buttons, and check boxes.

If a particular configuration option needs to prompt you for answers to several questions, those questions are now presented on a single Web page. After all of the questions are filled in, you should press the *Submit* button to send the data back to the IBM 8210 for validation.

The hierarchy of the Web browser interface is very similar to that of the command line interface.

History Function

The Web Configurator uses a selection list and a *Return to* button to provide an advanced history function. Depending upon your choice of HTML browser, a pick list, choice box or pull-down list box will be displayed. This list of selections contains the names of the pages visited under the current branch of the software structure. To return to a previously visited page within the current command pathway, select that entry from the list and click the *Return To* button.

Help System for the Web Browser Interface

Optional, free-of-charge, help files for the Web Browser interface can be downloaded from the Web. Use of the help button located at the bottom of Web Browser configuration panels requires the installation of these help files.

For download instructions and additional information about the help files, point your browser to URL `http://www.networking.ibm.com/nes/neshome.html`.

Quick Configuration Using the Web Browser Interface

Note: This section is most helpful when it is used while you are viewing the IBM 8210 Web interface.

Quick Configuration for the IBM 8210 using the Web interface is divided into the following steps:

- Guided configuration
- Devices
- LAN Emulation
- Bridging
- IP
- IPX
- LAN Emulation (MSS Client only)

Guided Configuration

To view the individual steps that are required for quick configuration, select **Guided Configuration** from the menu on Configuration and Console page 2, shown in

Figure 23 on page 62. On each step, you will be presented with a link that allows you to skip to the next step. When you submit the form for a step, the results page will contain a link that takes you to the next step in the guided configuration. The results page in the last step of the guided configuration contains a link to take you back to the home page.

If you complete the guided configuration, you will have been through every step of a quick configuration. If you want to change only certain aspects of a quick configuration, use each of the separate steps. For example, to change only LAN emulation parameters, select that step.

Devices

Selecting **Devices** presents a list of the currently configured devices, which are the ATM devices. Select an interface and click on the **Submit** button to add the device using the next available network and slot numbers. A **Submit** button is included on the results page if there is still room to add more devices. A **Submit** will not be included on the results page once all the available slots have been filled, so it is impossible to attempt to add too many devices.

LAN Emulation

Selecting **LAN Emulation** presents a form that allows the LAN Emulation Configuration Server (LECS), LAN Emulation Server (LES), Broadcast Manager, and LAN Emulation Client (LEC) to be configured for each ATM device that has been added.

When you add multiple ATM devices, radio buttons are presented that allow you to configure the ATM device that the LECS will use.

For each ATM device that you add, you have the option of adding one emulated token ring, one emulated Ethernet, neither or both. Each emulated LAN (ELAN) is added by selecting its associated check box. For each ELAN that you configure, you must specify the name and selector to be used by the LES. You can also specify which types of broadcast management will be performed by selecting the appropriate check boxes for:

- IP
- IPX
- NetBIOS
- Source Routing (token-ring ELANs only)

When you click on the Submit button, all of the LAN Emulation components are configured based on the input from the form. A LES is added for each ELAN. The LESs are configured to use the burned-in ESI of the ATM device along with the selector byte that you previously specified for the ELAN.

Broadcast management is configured for each ELAN as specified by the check boxes from the form.

An LE client is also added for each ELAN. The clients are configured to request the ELAN name configured from the form and to use the burned-in ESI of the ATM device along with a selector byte automatically generated by the system.

The LECS is configured with policies for the ELAN by name and for the ELAN by type. ELAN by name is given the highest priority. When a LE client joins and specifies one of the configured ELAN names, it will be sent to the appropriate LES. Clients joining an ELAN by type will be sent to the LES of the desired type that is on the ATM device that the LECS is configured to use.

When you submit the form by clicking on the Submit button, LAN emulation is configured according to the submitted data and the results are displayed on a new page. Quick configuration allows you to configure only one ELAN per ATM device. If you need to configure additional ELANs, click on the links that are included on this page to provide links to the more detailed configuration pages for the LECS and each LES and LE client.

When you are done with this step, all ELAN interfaces have been added to the configuration. This step combined with the previous step provides the network interfaces necessary for performing bridging, IP, and IPX configuration in the subsequent steps.

Bridging

Selecting **Bridging** presents a form that allows bridging to be configured on each network interface that can support bridging. You can also configure the bridge parameters required for source route bridging, which include the bridge number and the virtual segment number. For each emulated token-ring interface capable of bridging, you are given the option to enable source routing and to configure a segment number if source route bridging is enabled.

When the form is submitted by clicking on the Submit button, transparent bridging is automatically enabled for all token-ring and Ethernet LE clients. Bridging can be done only on the LE clients and not directly on the ATM devices. The results are displayed on a new page.

IP

Selecting **IP** presents a form that allows IP to be configured on each network interface. For each interface, enable IP by selecting the associated check box. When enabling IP, provide an IP address and mask using the dotted decimal format. The IP address and the subnet mask are the only parameters required to enable IP on an ELAN.

When enabling IP on an ATM device, you are actually configuring Classical IP (RFC 1577). In this case, select a radio button to choose between a *client-only* configuration or a *client and server* configuration. If you select *client-only*, specify the 20-byte ATM address of the remote ARP server that the client will use. If you select *client and server*, specify the selector. The burned-in ESI and the specified selector make up the portion of the ATM address that can be configured.

Note: For quick configuration, the burned-in ESI is the only choice. You are required to set the selector.

When the form is submitted by clicking on the Submit button, IP is configured according to the submitted data and the results are displayed on a new page.

IPX

Selecting **IPX** presents a form that allows IPX to be configured on each network interface that can support IPX. Each eligible interface can be enabled for IPX by selecting the associated check box. If you enable IPX, configure a network number and select the encapsulation type to be used by choosing the appropriate value from the select list presented for each interface.

When you submit the form by clicking the Submit button, IPX is configured according to the submitted data and the results are displayed on a new page.

An Example of Quick Configuration Using the Web Browser Interface

The following procedure shows how to use Quick Configuration to configure LAN emulation using the Web Browser interface:

1. Connect to the IBM 8210 using a SLIP connection. Configure your SLIP stack to use 10.1.1.2 as the IP address of the IBM 8210 and 10.1.1.3 as your IP address.
2. Open the following URL: http://10.1.1.2/
3. From the MSS home page, click **Configuration and Console**.
4. From Configuration and Console click **Quick Configuration**.
   a. Click **LAN Emulation**.

      Change ELAN names if desired, and then click **Submit**.

      LES/BUS, LEC and LECS are now configured for one Token-Ring and one Ethernet ELAN. Either or both ELANs can be omitted if desired.

      LEC is now configured for one Token-Ring and one Ethernet ELAN. Either or both ELANs can be omitted if desired.

      Select **Quick Configuration** from the Command History and click **Return to**.

   b. Click **IP**.

      Enable IP on the desired interfaces. IP must be enabled on at least one interface. The choices are:

      - Enabling Classical IP on the ATM adapter interface
      - Enabling IP on each of the ELAN interfaces defined in the previous step

      Change the IP addresses and masks to appropriate values for your network.

      If Classical IP is configured as a client only, the ATM address of the ARP Server must be entered.

      Click **Submit**.

      IP is now configured on the specified interfaces.

      Click the home icon at the bottom of the screen.
5. From the MSS home page, click **Configuration and Console**.

   From Configuration and Console click **Router Configuration**

   Click **RELOAD**.

   Select **Yes** and click the **Submit** button to restart the IBM 8210.

The IBM 8210 will now be accessible from the network using the IP addresses that were specified in step 4.b.

Chapter 6. MSS Server Voice/Data/Fax Modem Support

A PCMCIA Voice/Data/Fax Modem is shipped with the MSS Server in the U.S. and Canada; in most other countries, the PCMCIA Data/Fax Modem is shipped. Check with your IBM representative if you want to determine whether you will receive the Data/Fax Modem.

If you do not use the Voice/Data/Fax Modem or the Data/Fax Modem, you can purchase a modem and attach it externally to the EIA 232 port for remote access to the MSS Server. Information about the types of modem supported is found in the *IBM Multiprotocol Switched Services (MSS) Server Introduction and Planning Guide,* GC30-3820.

Installation of the Voice/Data/Fax Modem

Follow these steps to install the Voice/Data/Fax Modem:

1. Use the eject button to remove the Data/Fax Modem, if it is present.
2. Insert the Voice/Data/Fax Modem in the available PCMCIA slot.

The Voice/Data/Fax Modem is hot-pluggable. It will re-initialize when it is inserted in the PCMCIA slot.

If you use the serial service port at the same time that you use the Voice/Data/Fax Modem or the Data/Fax Modem, you need an analog telephone line for each connection.

Data/Fax Modem

This PCMCIA modem allows remote connection of a workstation to the MSS Server over telephone lines to access the command line interface, the Web browser interface, or the Configuration Program. You must use serial line Internet protocol (SLIP) over the telephone line to access the Configuration Program.

In addition, it can be configured to fax a report whenever the MSS Server sends an alert. See “Voice Pager Messages” on page 70 for a example of the kinds of alerts that the Data/Fax Modem sends.

Neither the Data/Fax Modem nor the Voice/Data/Fax Modem require any special configuration.

MSS Server Voice Access Using the Voice/Data/Fax Modem

When you place a voice call to the Voice/Data/Fax Modem, you will hear a voice menu. Items on this menu will allow you to access the MSS Server and to exercise limited control over it. The four capabilities enabled by the Voice/Data/Fax Modem are:

1. Performance monitoring
2. Remote problem determination
3. Network monitoring
4. Limited configuration

© Copyright IBM Corp. 1996, 1998

MSS Server Voice/Data/Fax Modem Support

The Voice/Data/Fax Modem lacks speech synthesis, so verbal output is limited to the capabilities of the prerecorded voice files. The model implemented for the MSS Server uses a fax machine as an output device and the telephone primarily as an input device. You press a touch-tone telephone key to give information to the MSS Voice Response Unit.

As a result, most of the information obtained from the Voice/Data/Fax Modem is in the form of faxed reports. Files containing the report information will be constructed and passed to the fax function.

Performance Information

A menu option that provides selected performance information and predefined performance and configuration reports is available using the Voice/Data/Fax Modem.

Remote Service

For remote service, the Voice/Data/Fax Modem provides a menu of activities that the caller can utilize, including:

- Resetting the MSS Server
- Reviewing pager log entries
- Reviewing nonvolatile memory log entries
- Obtaining a report on field replaceable unit (FRU) status

Network Monitoring

Network monitoring is generally provided using SNMP input that is handled by a network manager. However, the Voice/Data/Fax Modem provides some limited ability to access or retrieve information for the caller. The following menus are offered:

- Network management statistics and information
- Predefined reports available using fax

Configuration

The Voice/Data/Fax Modem allows you to change a limited number of configuration parameters. See “Option 5—Configuration” on page 73 for more information.

Important: Exercise caution when you use the voice menu to change configuration parameters. Changes to the configuration that are made using the voice menu cause the current configuration to be written directly to static random access memory (SRAM). When these changes are written to SRAM, any temporary changes that have been made using the Web browser interface or the command line interface are also written to SRAM and become part of the active configuration. Before you use the voice menu to change any parameters, you should make sure that all temporary parameter settings are acceptable.

MSS Server Voice Pager Support

The voice pager is included as a way to alert you that there is a problem, for example, that the MSS Server has become overheated or has had to reload due to an unrecoverable error of the software.

The voice pager function can call a telephone number and deliver a voice message describing a problem. The pager attempts to detect that the telephone has been answered before it speaks the message. It can speak its message to a person, a voice mail system, or a voice paging service. It cannot determine which of these methods was used to answer the telephone.

You can configure multiple telephone numbers to receive the pager messages. The pager will try them in sequence until one answers. Whenever one of the numbers is answered, the pager message is considered delivered.

Voice Pager Configuration Parameters

You can control the sending of outbound telephone call page messages. These are the paging parameters:

- PagerNum character strings

  These are the telephone numbers to call for the outbound voice messages generated by problem conditions. The telephone numbers will be called until one answers so that the voice message can be delivered. You can have from zero to 4 numbers. If there are zero telephone numbers, outbound page messages will not be attempted.

  – Quantity of telephone numbers
    - Maximum 4
    - Minimum 0
    - Default 0 (no telephone numbers)

  – Length of the telephone number
    - Maximum 64
    - Minimum 0
    - Default 0 (no telephone number)

  – Content of the telephone number

    The telephone numbers can contain digits 0 through 9 and commas. A comma will cause the outbound dialer to pause for 2 seconds. This feature is often used when dialing an outside line or calling a second number.

- Retry Interval integer

  High-severity voice page messages will be sent until the machine is called by the receiver of the message and the receipt of the page message is acknowledged. This parameter gives the time in minutes to wait before re-sending the voice page message. This parameter is known as the *nag interval*. If this number is zero, high-severity page messages will be sent only once.

  – Length of minutes in the retry interval

    This parameter specifies the length of time during which the pager will continue to re-send high-severity voice messages.
    - Maximum 840 (24 hours)
    - Minimum 0
    - Default 60 (1 hour)

Voice Pager Messages

All page messages start with the same prefix:

```
This is a message from an IBM MSS Server serial number nnnnnnnn
```

The page prefix message will be followed by a unique problem message. Currently, there are three problem messages that the pager will deliver:

1. The MSS Server has rebooted due to an unrecoverable error.
2. The MSS Server is over recommended operating temperature. Further temperature increases may cause the MSS Server to shut down.
3. The MSS Server has exceeded maximum operating temperature and is shutting down.

Maintenance Log

The maintenance log keeps a record of fax and paging activity. The log entries are time-stamped. The log can be sent to a fax machine for viewing.

Maintenance Log Configuration Parameter

You can control the size of the maintenance log. This log is a wrap-around file that never changes size. If the file is defined to have 100 entries, it will be created to contain 100 entries. When the log is filled, the oldest log entry will be replaced. Each log file entry takes approximately 250 bytes of disk space.

The configuration parameter is an integer—MaintenanceLogSize— that specifies the number of log entries contained in the file.

- Maximum 4096
- Minimum 32
- Default 64 (16 000 bytes disk space)

Voice/Data/Fax Modem Menu Items

When the Voice/Data/Fax Modem receives a call, it requests that the caller press the pound (#) key. If the # is pressed, the Voice/Data/Fax Modem recognizes that this is a voice call. The voice menu takes control and requests the MSS Server personal identification number (PIN).

Note: The default value for this PIN is 8210001. Whichever PIN is configured first is the supervisory PIN. If only one PIN is configured, it is the supervisory PIN. If you configure one PIN and delete 8210001, then the PIN that you have configured becomes the supervisory PIN.

Each additional PIN that is configured is placed in a sequence. For example, if you configured three PINs, and then deleted the default PIN and the first PIN, the second PIN would become the supervisory PIN.

Note: At this point, the functions offered by the Voice/Data/Fax Modem are the same as certain functions that you can access using the command line interface. Refer to the two volumes of the *Command Line Interface User's Guide and Protocol Reference* for more information about these functions. In the description of the Voice/Data/Fax Modem menu that follows, keywords

from the command line interface are provided to help you find the relevant information in the *Command Line Interface User's Guide and Protocol Reference*.

The main voice menu offers the following options:

Voice Message
Function

Press 1 to reset
MSS Server Reset

Press 2 for operational statistics
Status and statistics

Press 3 for router protocol reports
Reports

Press 4 for event log reports
Event logs

Press 5 for configuration options
Configuration

Press 6 for device presence and status
Device presence and status report

Press 7 to resend last fax report
Resend fax

Press 8 for disconnect call
Disconnect

Press 9 for repeat menu
Repeat menu

The options are repeated approximately every 15 seconds until a valid entry is made or until the call has been terminated.

Option 1—Reset

When you use the Voice/Data/Fax Modem to perform a reset, you are prompted to confirm that you want to perform the reset. If you do not confirm the reset, the main menu is repeated. If you do confirm the reset, the voice message responds, "The MSS Server will be reset". Your connection to the MSS Server is then broken and the reset occurs.

Attention: A reset interrupts the function of the MSS Server for up to 90 seconds. Be sure that the network is prepared for the interruption.

Option 2—Status and Statistics

Statistics are available from several sources. The following general MSS Server statistics will be packaged as a single report and faxed upon request.

1. Status of Micro Operating System (MOS) processes (as reported by the *STATUS* keyword from the MOS operator console)
2. Memory
   - Number of bytes (as reported by the *MEMORY* keyword from the MOS operator console)

- Heap and buffer memory (as reported by the *MEMORY* keyword from the configuration gateway [CGW] console)
- Network interface buffers (as reported by the *BUFFER* keyword from the CGW console)

3. Interface (as reported by the *INTERFACE* keyword from the CGW console)
4. Network (as reported by the *STATISTICS* keyword from the CGW console)
5. Uptime (as reported by the *UPTIME* keyword from the CGW console)
6. Queue length (as reported by the *QUEUE* keyword from the CGW console)
7. Error counts (as reported by the *ERROR* keyword from the CGW console)
8. Event Logging Statistics (as reported by the *STATISTICS* keyword from the *EVENT* keyword from the CGW console)
9. Gateway configuration (as reported by the *CONFIGURATION* keyword from the CGW console)
10. Log level (as reported by the *LOG* keyword from the CGW console)
11. Code image and configuration information (available and active)
12. Thermal status of the hardware

When you request *Status and statistics*, you will hear one of these two messages: “MSS Server statistics will be faxed.” or “Statistics not available.” If you do not disconnect the call, the voice menu starts again.

Option 3—Reports

You can also request protocol reports other than statistics from the voice menu.

- IP

  The following IP information will be provided in a report:

  – Access control list (as reported by the *ACCESS* keyword from IP from PROTOCOL on the CGW console)
  – Address cache (as reported by the *CACHE* keyword from IP from PROTOCOL on the CGW console)
  – Counter values (as reported by the *COUNTERS* keyword from IP from PROTOCOL on the CGW console)
  – Interface addresses (as reported by the *INTERFACE* keyword from IP from PROTOCOL on the CGW console)
  – Table, buffer, cache sizes (as reported by the *SIZES* keyword from IP from PROTOCOL on the CGW console)
  – Static routes (as reported by the *STATIC* keyword from IP from PROTOCOL on the CGW console)

- IPX
  – Interface addresses (as reported by the *CONFIG* keyword from IPX from PROTOCOL on the CGW console)
  – Cache information (as reported by the *CACHE* keyword from IPX from PROTOCOL on the CGW console)
  – Counters (as reported by the *COUNTERS* keyword from IPX from PROTOCOL on the CGW console)

- LAN emulation (as reported by the *LIST* keyword from LE-SERVICES from ATM from NETWORK on the CGW console)
  – LES/BUS Pairs (as reported by the *LIST* keyword from LE-SERVICES from ATM from NETWORK on the CGW console; an ATM interface must have been selected)

- Bridging
  - Brief universal summary of the state of the bridge (as reported by the *LIST BRIDGE* keywords from ASRT from PROTOCOL on the CGW console)

When you choose *Reports*, you will be prompted to select the protocol report option. Select IP, IPX, LAN Emulation, or bridging. Then you will hear either “Report not available” or “MSS Server Protocol Report will be faxed.” If you do not disconnect the call, the voice menu starts again.

Option 4—Event Logs

The MSS Server maintains several logs. Information contained there may be of interest to the systems administrator.

- Nonvolatile memory error log (accessed through the firmware log interface)
- Operational diagnostics log (using the Diagnostics Control System interface)
- Pager log entries (new)

Note: MSS Server trouble reports (critical problems) can be automatically faxed. These reports are not part of the voice menu structure.

When you choose *Event logs*, you will hear the voice message “MSS Server event logs will be faxed.” or “Event logs not available.” If you do not end the call, the voice menu starts again.

Option 5—Configuration

The Voice/Data/Fax Modem provides a limited configuration input capability. You can access the following configuration options using the Voice/Data/Fax Modem:

- Fax telephone number (up to 64 digits)
- Thermal shutdown mode (enabled or disabled)—Standalone MSS Server only
- Auto-Fax for trouble reports (On or Off)
- Pager telephone numbers (up to 64 digits)
- Personal identification number (PIN) maintenance

The functions of the Voice/Data/Fax Modem are protected by up to 10 personal identification numbers. Any person with knowledge of the supervisory PIN can add, delete, or modify PINs. The supervisory PIN is the first one in the list of 10 allowed PINs.

Note: The Voice/Data/Fax Modem is shipped with a default supervisory PIN of 8210001.

When you choose *Configuration*, you will hear the voice message “Change Voice/Data/Fax Modem PINs.” Then, you are prompted to add, delete, or change the PINs. When you are done, if you do not disconnect the call, the voice menu starts again.

Option 6—Device Presence and Status Report

Remote service is normally provided over the TTY or SLIP interface. In addition to the reporting and reset capabilities previously described, you can request a report that provides detailed device presence and status (DPS) information. This information can be obtained in a verbal message or in a more detailed fax report.

The verbal message begins with a statement of the number of recognized devices followed by a statement of the number of those that are enabled. If any are disabled, it will then state the number disabled. Finally, if any are out of service for other reasons, it will state the number of devices in non-operational states other than disabled.

Device presence and status fax reports contain the same information that is accessible when you select the *DIAGS* keyword from the MOS operator control and then select Option 1, Device Status, from the DIAGS menu.

You can also obtain this information from the Web browser interface by selecting *Diagnostics* from the main menu.

Option 7—Resend Last Fax Report

You should request this option before you select another fax report because the previous fax report file is recreated for each call. If you make this request before you request the next fax report, the file for the previous call is retained and any additional requests will be appended to it.

Option 8—Disconnect Call

You can request that the modem disconnect the call. When you choose *Disconnect call*, you will hear the voice message “Are you sure you want to disconnect?” and you will be prompted to respond. If you do not disconnect the call, the voice menu starts again.

Option 9—Repeat Menu

You can request a repetition of the menu.

Chapter 7. The OPCON Process and Commands

This chapter describes the OPCON interface configuration and operational commands. It includes the following sections:

- "What is the OPCON Process?"
- "Accessing the OPCON Process"
- "OPCON Commands"

What is the OPCON Process?

The Operator Console process (OPCON) is the root-level process of the router software user interface. The main function of OPCON is to communicate with processes at the secondary level, such as Configuration, Console, and Event Logging. Using OPCON commands, you may also:

- Display information about device memory usage
- Reload the device software (reboot)
- Telnet or ping to other routers or hosts
- Display status information about all router processes
- Manipulate the output from a process
- Change the OPCON intercept character

Accessing the OPCON Process

When the router starts for the first time, a boot message appears on the console. Then the OPCON prompt (*) appears on the console, indicating that the OPCON process is active and ready to accept commands.

The OPCON process allows you to configure, change, and monitor all of the router's operating parameters. While in the OPCON process, the router is forwarding data traffic. When the router is booted and enters OPCON, a copyright logo and an asterisk (*) prompt appears on the locally attached console terminal. This is the OPCON (OPerator's CONsole) prompt, the main user interface that allows access to second-level processes.

Some changes to the router's operating parameters made while in OPCON take effect immediately without requiring reinitializing of the router. If the changes do not take effect, use the **reload** command at the * prompt.

At the * prompt, an extensive set of commands enables you to check the status of various internal software processes, monitor the performance of the router's interfaces and packet forwarders, and configure various operational parameters.

OPCON Commands

This section describes the OPCON commands. Commands that are needed more often appear before the "- - - - -" separator. Each command includes a description, syntax requirements, and an example. The OPCON commands are summarized in Table 4 on page 76. To use them, access the OPCON process and enter the appropriate command at the OPCON prompt (*).

© Copyright IBM Corp. 1996, 1998

Table 4. OPCON Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Configuration*	Accesses the device’s configuration process. (`talk 6`)
Console*	Accesses the device’s console process. (`talk 5`)
Event Logging System*	Accesses the device’s event logging process. (`talk 2`)
ELS Console*	Accesses the device’s secondary ELS Console process. (`talk 7`)
Logout	Logs off a remote console.
Ping	Pings a specified IP address.
Reload	Reloads the device.
Telnet	Connects to another device.
- - - - - -	- -
Diags	Displays device status and the contents of the hardware test log and the hardware error log.
Divert	Sends the output from a process to a console or other terminal.
Flush	Discards the output from a process.
Halt	Suspends the output from a process.
Intercept	Sets the OPCON default intercept character.
Memory	Reports the router’s memory usage.
Status	Shows information about all router processes.
Talk	Connects to another router process and enables the use of its commands.

***:** When you use this command for the first time, you will be reminded that you can use **Ctrl-P** to return to the MOS Operator Console prompt (*).

Configuration

Use the **configuration** command to access the device’s configuration process (`talk 6`). See “Chapter 8. The CONFIG Process (CONFIG - Talk 6) and Commands” on page 85 for more information.

Syntax:

configuration

Example:

```
* configuration

(To return to the MOS Operator Console prompt (*), press Control-P)

Gateway user configuration
Config>
```

Console

Use the **console** command to access the device’s console and monitoring process (`talk 5`). See “Chapter 11. The Operating/Monitoring Process (GWCON - Talk 5) and Commands” on page 129 for more information.

Syntax:

console

Example:

```
* console

CGW Operator Console

+
```

Diags

Use the **diags** command to display the Diagnostic Main Menu. The diagnostic menus allow you to enable, disable and test hardware adapters or ports. Diagnostic menus have on-screen help for the various options and status information that is available.

You can use the “b” (back) key to return to any previous menu. Use the “e” (exit) key to exit the diagnostics and return to the OPCON command prompt.

Syntax:

diags

Divert

Use the **divert** command to send the output from a specified process to a specified terminal. This command allows you to divert the output of several processes to the same terminal to simultaneously view the output. The **divert** command is commonly used to redirect MONITR output messages to a specific terminal. The router allows only certain processes to be redirected.

The **divert** command requires the PID and tty# (number of the output terminal). To obtain these values, use the OPCON **status** command. The terminal number can be the number of either the local console (tty0) or one of the remote consoles (tty1, tty2). The following example shows Event Logging System messages generated by the MONITR process (2) being sent to a remote console *tty1* (1).

Event messages are displayed immediately even though you may be in the middle of typing a command. The display and keyboard have separate buffers to prevent command confusion. The following example shows the MONITR process connected to TTY0 after executing the **divert 2 0** command. If you want to stop the output, enter **halt 2**. The **halt** command is described in “Halt” on page 78.

Syntax:

divert *pid tty#*

Example:

```
* divert 2 0
* status
Pid  Name      Status TTY  Comments
1    COpCon    IDL    TTY0
2    Monitr    IDL    TTY0
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    ELSCon    DET     --
8    ROpCon    IDL    TTY1
9    ROpCon    RDY    TTY2 jlg@128.185.40.40
10   WEBCon    IDL    --
```

Els

Use the **els** command to access the device's secondary ELS console process, (`talk 7`). See "Accessing the Secondary ELS Console Process, ELSCon (Talk 7)" on page 15 for more information.

Syntax:

els

Event

Use the **event** command to access the device's event logging process, (`talk 2`). See "Chapter 13. Using the Event Logging System (ELS)" on page 145 for more information.

Syntax:

event

Flush

Use the **flush** command to clear the output buffers of a process. This command is generally used before displaying the contents of the MONITR's FIFO buffer to prevent messages from scrolling off the screen. Accumulated messages are discarded.

The router allows only certain processes to be flushed. To obtain the *pid* and *tty#*, use the OPCON **status** command. In the following example, after executing the **flush 2** command, the output of the MONITR process is sent to the Sink (it has been flushed).

Syntax:

flush *pid*

Example:

```
* flush 2
* status
Pid  Name      Status TTY  Comments
1    COpCon    IDL    TTY0
2    Monitr    IDL    Sink
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    ELSCon    DET     --
8    ROpCon    IDL    TTY1
9    ROpCon    RDY    TTY2 jlg@128.185.40.40
10   WEBCon    IDL    --
*
```

Halt

Use the **halt** command to suspend all subsequent output from a specified process until the **divert**, **flush**, or **talk** OPCON command is issued to the process. The router cannot redirect all processes. **Halt** is the default state for output from a process. To obtain the PID for this command, use the OPCON **status** command. In

the following example, after executing the **halt 2** command, the MONITR process is no longer connected to TTY0. Event messages no longer appear.

Syntax:

halt *pid*

Example:

```
* halt 2
* status
Pid  Name      Status TTY  Comments
1    COpCon    IDL    TTY0
2    Monitr    IDL     --
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    ELSCon    DET     --
8    ROpCon    IDL    TTY1
9    ROpCon    RDY    TTY2 jlg@128.185.40.40
10   WEBCon    IDL    --
```

Intercept

Use the **intercept** command to change the OPCON intercept character. The intercept character is what you enter from other processes to get back to the OPCON process. The default intercept key combination is **Ctrl-P**.

The intercept character ***must*** be a control character. Enter the ^ (shift 6) character followed by the letter character you want for the intercept character.

Syntax:

intercept ^ *character*

Example:

```
* intercept ^a
```

From this example, the intercept character is now **Ctrl-A**.

Logout

Use the **logout** command to terminate the current session for the user who enters the logout command. If the console login is enabled, this command will require the next user to log in using an authorized userid/password combination. If the console login is not enabled, the OPCON prompt appears again.

Syntax:

logout

Memory

Use the **memory** command to obtain and display information about the router's global heap memory usage. The display helps you to determine if the router is being utilized efficiently. For an example of memory utilization, see Figure 24 on page 80.

See "Memory" on page 136 for memory usage via talk 5.

Syntax:

memory

Example:

```
* memory
Number of bytes:  Busy = 319544, Idle = 1936, Free = 1592
```

Busy Specifies the number of bytes currently allocated.

Idle Specifies the number of bytes previously allocated but freed and available for reuse.

Free Specifies the number of bytes that were never allocated from the initial free storage area.

Note: The sum of the Idle and Free memory equals the total available heap memory.

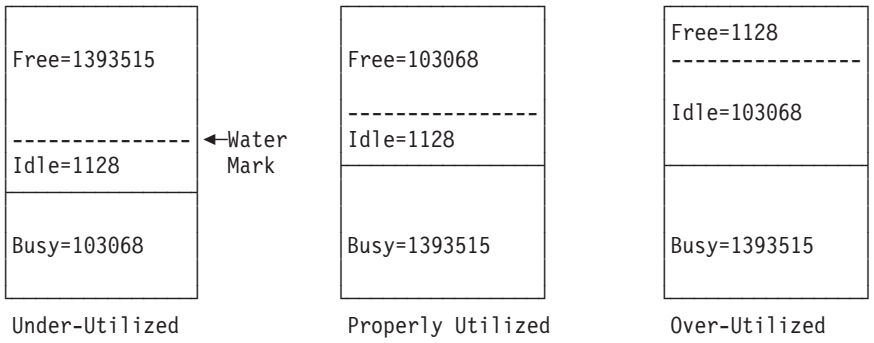


Figure 24. Memory Utilization

Ping

Use the **ping** command to have the router send ICMP Echo messages to a given destination (that is, “pinging”) and watch for a response. This command can be used to isolate trouble in the internetwork.

Syntax:

ping *dest-addr [src-addr data-size ttl rate tos data-value]*

The ping process is done continuously, incrementing the ICMP sequence number with each additional packet. Each matching received ICMP Echo response is reported with its sequence number and the round-trip time. The granularity (time resolution) of the round-trip time calculation is usually around 20 milliseconds, depending on the platform.

To stop the ping process, type any character at the console. At that time, a summary of packet loss, round-trip time, and number of unreachable ICMP destinations will be displayed.

When a broadcast or multicast address is given as destination, there may be multiple responses printed for each packet sent, one for each group member. Each returned response is displayed with the source address of the responder.

You can specify the size of the ping (number of data bytes in the ICMP message, excluding the ICMP header), value of the data, time-to-live (TTL) value, rate of pinging, and TOS bits to set. You can also specify the source IP address. If you do not specify the source IP address, the router uses its local address on the outgoing interface to the specified destination. If you are validating connectivity from any of the router's other interfaces to the destination, enter the IP address for that interface as the source address.

Only the destination parameter is required; all other parameters are optional. By default the size is 56 bytes, the TTL is 64, the rate is 1 ping per second, and the TOS setting is 0. The first 4 bytes of the ICMP data are used for a timestamp. By default the remaining data is a series of bytes with values that are incremented by 1, starting at X'04', and rolling over from X'FF' to X'00' (for example, X'04 05 06 07 . . . FC FD FE FF 00 01 02 03 . . .'). These values are incremented only when the default is used; if the data byte value is specified, all of the ICMP data (except for the first 4 bytes) is set to that value and that value is not incremented. For example, if you set the data byte value to X'FF', the ICMP data is a series of bytes with the value X'FF FF FF . . .'.

Example:

```
* ping
Destination IP address [0.0.0.0]? 192.9.200.1
Source IP address [192.9.200.77]?
Ping data size in bytes [56]?
Ping TTL [64]?
Ping rate in seconds [1]?
Ping TOS (00-FF) [0]? e0
Ping data byte value (00-FF) [ ]?
PING 192.9.200.77-> 192.9.200.1:56 data bytes,ttl=64,every 1 sec.
56 data bytes from 192.9.200.1:icmp_seq=0.ttl=255.time=0.ms
56 data bytes from 192.9.200.1:icmp_seq=1.ttl=255.time=0.ms
56 data bytes from 192.9.200.1:icmp_seq=2.ttl=255.time=0.ms


----192.9.200.1 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max=0/0/0 ms
```

Reload

Use the **reload** command to reboot the router by loading in a new copy of the router software. When you use this command from a remote console, you install a new software load without going to the router. This command executes the same functions as pressing the reset button except that the router will not dump (if so configured). Before the reload takes effect, you are prompted to confirm the reload. You are also prompted if you have not saved the configuration changes.

Syntax:

reload

Example:

```
* reload
Are you sure you want to reload the gateway (Yes or No)?
```

Status

Use the **status** command to display information about all router processes. By entering the PID after the **status** command, you can look at the status of only the desired process. The following example shows the total status display.

Syntax:

status *pid*

Example:

```
* status
Pid  Name      Status TTY  Comments
1    COpCon    IDL    TTY0
2    Monitr    IDL     --
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    IOW     --
6    Config    IOW    TTY1
7    ELSCon    DET     --
8    ROpCon    IOW    TTY1 128.185.46.101
9    ROpCon    RDY    TTY2 128.185.46.104
10   WEBCon    IDL    --
```

Pid Specifies the PID. This is the process to talk to from OPCON, or it can be an argument to the STATUS command to request status information about a specific process.

Name Specifies the process name. It usually corresponds to the name of the program that is running in the process.

Status

Specifies one of the following:

IDL Specifies that the process is idle and waiting for completion of some external event, such as asynchronous I/O.

RDY Specifies that the process is ready to run and is waiting to use the CPU.

IOW Specifies that the process is waiting for synchronous I/O, usually its expected standard input, to complete.

DET Specifies that the process has output ready to be displayed and it is either waiting to be attached to a display console or waiting to have its output diverted to a specified console.

FZN Specifies that the process is frozen due to an error. This usually means the process is trying to use a device which is faulty or incorrectly configured.

TTY*n* Specifies the output terminal, if any, to which the process is currently connected.

TTY0 Local console

TTY1 or TTY2

Telnet consoles.

Sink Process has been flushed.

Two dashes (--)

Process has been halted.

Comments

Specifies the user's login IP address provided during login when a user is logged in using Telnet (ROpCon).

Talk

You can use the **configuration**, **console**, or **event** comands to connect to other processes, such as CONFIG, GWCON, or MONITR, or use the **talk** command.

After connecting to a new process, you can send specific commands to and receive output from that process. You cannot talk to the TASKER or OPCON processes.

To obtain the PID, use the OPCON **status** command. Once you are connected to the second-level process, such as CONFIG, use the intercept character, **Ctrl-P**, to return to the * prompt.

Syntax:

talk *pid*

Example:

```
* talk 5

CGW Operator Console

+
```

When using third-level processes, such as `SNMP Config>` or `SNMP>`, use the **exit** command to return to the second level.

Telnet

Use the **telnet** command to remotely attach to another router or to a remote host. The only optional parameter is the terminal type that you want to emulate.

You can use the **telnet** command with IPv4 or with IPv6 addresses.

A router has a maximum of five Telnet sessions: two servers (inbound to the router), and three clients (outbound from the router).

Note: To use Telnet in a pure bridging environment, enable Host Services.

Syntax:

telnet *ip-address terminal-type*

Example 1: `telnet 128.185.10.30` or **`telnet 128.185.10.30 23`** or **`telnet 128.185.10.30 vt100`**

```
Trying 128.185.10.30  ...
Connected to 128.185.10.30
Escape character is '^]'
```

When telneting to a non-existent IP address, the router displays:

```
Trying 128.185.10.30  ...
```

To enter the Telnet command mode, type the escape character-sequence, which is **Ctrl-]**, at any prompt.

```
telnet>
```

If you Telnet into a router,

- Press ← **Backspace** to delete the last character typed on the command line.

  Note: When using a VT100 terminal, do not press ← **Backspace** because it inserts invisible characters. Press **Delete** to delete the last character.
- Press **Ctrl-U** at the `telnet>` prompt to delete the whole command line entry so that you can reenter a command.

The Telnet command mode consists of the following subcommands:

close Close current connection

display
Display operating parameters

mode Try to enter line-by-line or character-at-a-time mode

open Connect to a site

quit Exit Telnet

send Transmit special characters ('send ?' for more)

set Set operating parameters ('set ?' for more)

status Print status information

toggle Toggle operating parameters ('toggle ?' for more)

z Suspend Telnet

? Print help information

The **status** and **send** subcommands have one of two responses depending on whether or not the user is connected to another host. For example:

Connected to a host:

```
   telnet>    status
Connected to 128.185.10.30    Operating in character-at-a-time mode.    Escape character is ^].

   telnet>    send ayt
```

Note: The send command currently supports only ayt.

Not connected to a host:

```
   telnet>    status
   Need to be connected first.

   telnet>    send ayt

   Need to be connected first.
```

Use the **close** subcommand to close a connection to a remote host and terminate the Telnet session. Use the **quit** subcommand to exit the **telnet** command mode, close a connection, and terminate a Telnet session.

```
telnet>    close
```

or

```
telnet>    quit

logout
*
```

Chapter 8. The CONFIG Process (CONFIG - Talk 6) and Commands

This chapter describes the CONFIG process configuration and operational commands. It includes the following sections:

- "What is CONFIG?"
- "Entering and Exiting CONFIG" on page 92
- "CONFIG Commands" on page 92

What is CONFIG?

The Configuration process (CONFIG) is a second-level process of the router user interface. Using CONFIG commands, you can:

- Set or change various configuration parameters
- Add or delete an interface to the hardware configuration
- Enter the Boot CONFIG command mode
- Enter the Quick Configuration mode
- Clear, list, or update configuration information
- Enable or disable console login
- Communicate with third-level processes, including protocol environments

Note: Refer to the chapter "Migrating to a New Code Level" in *Mulitprotocol Switched Services (MSS) Server Service and Maintenance Manual* for information about migrating to a new code level.

CONFIG lets you display or change the configuration information stored in the router's nonvolatile configuration memory. Changes to system and protocol parameters do not take effect until you reload the router software. (For more information, refer to the OPCON **reload** command in "What is the OPCON Process?" on page 75).

Note: You must enter the **write** command to save the changes in the device's flash memory.

The CONFIG command interface is made up of levels that are called modes. Each mode has its own prompt. For example, the prompt for the SNMP protocol is `SNMP config>`.

If you want to know the process and mode you are communicating with, press **Enter** to display the prompt. Some commands in this chapter, such as the **network** and **protocol** commands, allow you to access and exit the various levels in CONFIG. See Table 5 on page 92 for a list of the commands you can issue from the CONFIG process.

© Copyright IBM Corp. 1996, 1998

Config-Only Mode

Config-Only mode is entered if the configuration file that you are using is empty or no protocols are configured. Config-Only mode can also be entered manually to recover from an invalid configuration that is causing the router to crash during start-up.

Automatic Entry Into Config-Only Mode

Config-Only mode is entered if the router detects a problem during operation or during router initialization.

The following conditions cause the router to enter Config-Only mode:

- The software load does not match the device configuration. Specifically, an attempt is made to configure a device or data link that is not supported by the software load.
- Deletion of all router interface information.

If the router enters Config-Only mode because an unsupported device is configured:

- Change the device information to match the hardware installed in (and supported by) the router, or change the unsupported device to “null device”.
- Enter the **Reload** command from the `Config (only)>` prompt.
- The router will automatically enter OPCON (*).

Manual Entry Into Config-Only Mode

To enter Config-Only mode, do one of the following:

- Reload the router with no configuration.
- Reload the router with no interfaces configured.
- Reload the router with no protocols configured.

See “Chapter 3. Using MSS Server Firmware” on page 27 for more information.

Quick Configuration

Quick Configuration (Quick Config) provides a minimal set of commands that allow you to configure bridging protocols and routing protocols present in the router load. You can also configure an SNMP community with WRITE_READ_TRAP access. This is useful during initial setup because the configuration program uses SNMP SET commands to transfer the configuration.

Important: At least one network device must be configured before using quick config. To add a device, use the **add device** command at the `config(only)>` or `config>` prompt.

Quick Config complements the existing configuration process by offering a shortcut. This shortcut allows you to configure the minimum number of parameters for these bridging protocols and routing protocols without having to exit and enter the different configuration processes. The other parameters are set to selected defaults.

Situations that call for the router to be quickly configured are:

- Blank or corrupted configuration memory, such as when one of the following situations occurs:

  - The router is configured for the first time.
  - Voltage fluctuations caused corruption of configuration memory.
  - The CPU board, which contains the configuration memory chip, was replaced in the router.
- Demonstration purposes, for which the router needs to be quickly configured to demonstrate its capabilities.
- Bench-marking tests to get the tests going without having to learn the router's operating system commands.

Quick Config operates as follows:

- It asks a series of questions with default values.
- It offers a short-cut to the detailed configuration of the normal mode command set.

Quick Config sets a number of default parameters based upon how you answer the configuration questions. What cannot be configured with Quick Config can be configured using Config after exiting Quick Config.

You cannot delete Quick Config information from within Quick Config. However, you can correct information either by exiting and returning to Quick Config, or by entering the **reload** command as a response to some Quick Config questions.

For complete information on using the Quick Config software, see "Appendix A. Quick Configuration Reference" on page 495.

Manual Entry Into Quick Config Mode

You might want to run Quick Config manually to demonstrate the router's capabilities or to reconfigure dynamically to perform benchmark tests without having to learn the router's operating system commands.

To enter Quick Config, type **qconfig** at the `Config>` prompt.

Exiting from Quick Config Mode

To exit Quick Config, restart by entering **r** from any prompt. Follow the queries until you enter **no** and then enter **q** to quit. The router returns to either the `Config (only)>` or the `Config>` prompt.

Configuring User Access

The router configuration process allows for a maximum of 50 user names, passwords, and levels of permission. Each user needs to be assigned a password and level of permission. There are three levels of permission: *Administration, Operation,* and *Monitoring*.

For more information, see 94.

Technical Support Access

If you are the system administrator, when you add a new user for the first time, you are asked if you want to add Technical Support access. If you answer yes, Technical Support is granted the same access privileges that you have as system administrator.

The password for this account is automatically selected by the software and is known by your service representative. This password can be changed using the **change user** command; however, if you do change the password, customer service cannot provide remote support. For additional information on the use of the **change user** command, see “Change” on page 95.

Configuring Spare Interfaces

Occasionally, you may need to configure a new interface along with its bridging and routing protocols without having to restart the device. You can accomplish this by configuring a number of ***spare interfaces*** on your device. Spare interfaces are useful if:

- You are adding ATM LAN Emulation clients.

  Use spare interfaces to add Token-Ring or Ethernet ATM LAN Emulation clients to an existing ATM interface.

To configure a spare interface:

1. Access the CONFIG process by entering **configuration**.
2. Configure the number of spare interfaces for the device using the **set spare-interfaces** command.
3. Exit the CONFIG process by pressing **Ctrl-P**.
4. Reload the device.

Example:

```
* configuration
Config> set spare 2
Config>
*reload
Are you sure you want to reload the gateway? (Yes or [No]) yes
```

When the device reloads, the spare interfaces are installed as null devices.

To use one of the spare interfaces:

1. Access the CONFIG process by entering **configuration**.
2. Configure the spare interface by using the **net** command to configure the interface or add ATM LAN Emulation clients.
3. Configure the various protocols and features using the **protocol** and **feature** commands.
4. Exit the CONFIG process by pressing **Ctrl-P**.
5. Access the GWCON process by entering **console**.
6. Bring the new interface online to the network using the **activate** command.

The following example shows how to configure and activate a new ATM LAN Emulation Client on which the IP protocol is configured. The ATM LAN Emulation Client and IP configurations are not shown.

```
* configuration
Config> net 0
ATM User Configuration
ATM Config> le-client
ATM LAN Emulation Clients Configuration
LE Client config> add token-ring
Added Emulated LAN as interface 6
LE Client config> config 6
ATM LAN Emulation Client configuration
⋮
(Here you would configure the ATM LAN Emulation Client)
⋮
```

```
Token Ring Forum Compliant LEC Config> exit
LE Client config> exit
ATM Config> exit
Config> protocol ip
IP Conifg>
:
(Here you would configure IP on the ATM LAN Emulation Client)
:
IP Config> exit
Config> write
ctrl-p
* console
+ activate 6
Interface 6 activated successfully
```

Restrictions for Spare Interfaces

The **activate** command cannot be used to activate a new interface on the network under the following conditions:

- You have already entered a **delete interface** command. The device must be restarted if ***any*** interface has been deleted. You cannot delete a spare interface (indicated by ***null*** in list displays).
- The spare interface is the only interface that enables a protocol or feature. The protocol or feature must already be enabled on an existing interface before it can be used by a spare interface.
- The new spare interface has a header size or trailer size greater than the sizes for other interfaces.
- There is not enough memory to allocate receive buffers for the new interface.

In these cases, you must restart the device to bring the new interface online.

You can configure the following protocols on spare interfaces, but you cannot activate them on the network using the **activate** command:

- MARS

Note: When using the configuration program, use the following to work with spare interfaces:

1. Make the configuration changes for the spare interface on the device
2. Enter the **activate** command on the device to bring the spare interface, protocols, and features online
3. Retrieve the configuration using the configuration program
4. Save the retrieved configuration into the configuration program database

There are requirements for certain functions. These are:

APPN	To activate this protocol on a spare interface, you must first activate the interface and then configure the protocol on the activated interface.
BGP	Use the BGP **reset neighbor** command to activate new neighbors.
IPX	Use the **reset** command to activate static routes, static services, and filter lists on the spare interface.
Bridging	• Bridging was not already active. • NetBIOS filters are defined on the spare interface. • The spare interface caused a change to the bridge personality or behavior (for example, adding SR port to pure TB bridge.
IP	Use the reset IP command to bring configuration changes online for access-controls and packet-filters.

Resetting Interfaces

Occasionally, you might need to change the configuration of a network interface along with its bridging and routing protocols without restarting the device. The **reset** command allows you to disable a network interface and then enable it using new interface, bridging and routing configuration parameters.

The interface, protocols and features configuration parameters are changed using the CONFIG process (talk 6) commands. The talk 6 commands affect the contents of the configuration memory. The configuration changes are activated by issuing the GWCON process (talk 5) **reset** command.

To reset an interface:

1. Access the CONFIG process (talk 6).
2. Use the **net** command and other commands to change configuration parameters.
3. Use the **protocol** and **feature** commands to change the interface-based configuration parameters.
4. Exit the CONFIG process by pressing **Ctrl-P**.
5. Access the GWCON process (talk 5).
6. Use the **reset** command to reset the interface and the protocols and features on the interface.

Example:

```
* configuration
Config> net 0
ATM User Configuration
ATM Config> le-client
ATM LAN Emulation Clients Configuration
LE Client config> config 6

. . . change ATM LAN Emulation Client parameters . . .

Ethernet Forum Compliant LEC Config> exit
LE Client config> exit
ATM Config> exit

Config> protocol ipx
IPX Config>

. . . change IPX parameters on the ATM LAN Emulation Client . . .

IPX Config> exit
Config>
*console
+reset 6
Resetting net 6 Eth/1...successful
```

Note: When using the configuration program, do the following to make configuration changes to existing interfaces:

1. Make the configuration changes for the interface on the device
2. Enter the **reset** command to reset interface, protocol and feature parameters
3. Retrieve the configuration using the configuration program
4. Save the retrieved configuration into the configuration program database

Restrictions for Resetting Interfaces

The **reset** command cannot be used to reset a network interface if:

- You have already entered a **delete interface** command. The device must be reloadedif any interface has been deleted.
- You have configured a larger MTU.
- You have configured a routing protocol or bridging on the interface, but that routing protocol or bridging is not currently active in the device.

In these situations, you must reload the device to activate the configuration changes.

You can change the configuration parameters of the following types of interfaces, but you cannot activate the changes using the **reset** command:

- ATM

You must reload the device to activate these configuration changes.

You can change the configuration parameters of the following protocols and features, but you cannot activate the changes using the **reset** command:

- AppleTalk
- Vines
- MARS

You must reload the device to activate these configuration changes.

There are also requirements for certain functions. They are:

Bridging	• Bridging was not already active. • NetBIOS filters are defined on the interface you are resetting. • The reset interface caused a change to the bridge personality or behavior (for example, adding SR port to pure TB bridge.
BGP	Use the BGP **reset neighbor** command to activate neighbor configuration changes.
APPN	Use the **activate_new_config** command to activate configuration changes.
IPX	Use the IPX **reset** command to activate configuration changes for static routes, static services, and filter-lists.
SNMP	Use the SNMP **revert** command to activate configuration changes.

Using System Dumps

A useful tool for debugging problems with the 8210 is the system dump. The dump is a compressed snapshot that the system saves to the hard drive if one is present, or to a remote host on the network .

To configure dumping:

1. Specify which three dump files you will save. See page 108 for more information.

2. Specify whether you want dumping re-enabled after a dump occurs. See page 107 for more information.
3. Enable dumping on the 8210. See page 99 for more information.

You can view the status of system dumping or retrieve a dump from the system. See “System View” on page 111 and “System Retrieve” on page 110, respectively.

Entering and Exiting CONFIG

To enter the CONFIG process from OPCON and obtain the CONFIG prompt, enter the **configuration** command. Alternatively, you can enter the OPCON **talk** command and the PID for CONFIG. The PID for CONFIG is 6.

```
* configuration
```

or

```
* talk 6
```

The console displays the CONFIG prompt (`Config>`). If the prompt does not appear, press the **Enter** key again.

To exit CONFIG and return to the OPCON prompt (*), enter the intercept character. (The default is **Ctrl-P** .)

CONFIG Commands

This section describes each of the CONFIG commands. Each command includes a description, syntax requirements, and an example. The CONFIG commands are summarized in Table 5.

After accessing the CONFIG environment, enter the configuration commands at the `Config>` prompt.

Table 5. CONFIG Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds an interface to the router configuration, or a user to the router.
Boot	Enters Boot CONFIG command mode.
Change	Changes a user’s password or a user’s parameter values associated with this interface. Also changes a slot/port of an interface.
Clear	Clears configuration information.
Delete	Deletes an interface from the router configuration or deletes a configured user. Also deletes system dump files.
Disable	Disables command completion, login from a remote console, system memory dumping and rebooting, or a specified interface.
Enable	Enables command completion, login from a remote console, system memory dumping and rebooting, or enables a specified interface.
Event	Enters the Event Logging System configuration environment.
Feature	Provides access to configuration commands for independent router features outside the usual protocol and network interface configuration processes.
List	Displays system parameters, hardware configuration, a complete user list.

Table 5. CONFIG Command Summary (continued)

Command	Function
Load	Lists, adds, or deletes optional software packages.
Network	Enters the configuration environment of the specified network.
Patch	Modifies the router's global configuration.
Performance	Provides a snapshot of the main processor utilization statistics.
Protocol	Enters the command environment of the specified protocol.
Qconfig	Initiates the Quick Config process.
Set	Sets system-wide parameters for buffers, host name, inactivity timer, packet size, prompt level, number of spare interfaces, dump parameters, location, and contact person.
System Retreive	Retrieves dumps
System View	Displays the dump settings and the current dump status. Also displays a summary of the dumps.
Time	Keeps track of system time and displays it on the console.
Unpatch	Restores patch variables to default values.
Write	Writes the current configuration information to the nonvolatile memory.

Add

Use the **add** command to add an interface to the configuration, or user-access. This command also recreates device records if the configuration is inadvertently lost.

Syntax:

add device
user . . .

device *device_type additional-config-info*

With the **add device** command, you must enter the interface device type (*device_type*). You are prompted for additional configuration parameters. This additional information varies by device and platform. Refer to "Accessing Network Interface Configuration and Operating Processes" on page 16 for additional information about device type and configuration parameters.

Note: If you are adding more than one interface, the order in which you add them is important because the router assigns a sequential interface number to the device when it is added. This interface number is an index number in the device list; it links the device with other protocol configuration information, such as the IP addresses associated with the device. (For more information, refer to the **list devices** command, "List" on page 102.)

All device and protocol configuration information related to network interfaces is stored by interface number. Any changes made to interface numbers will invalidate much of the device configuration information in the protocols.

Example:

```
add device atm
Device Slot x(0-3) 0?
Adding CHARM ATM Adapter device in slot 0 port 1 as interface x
(where x is the interface number assigned)
```

To determine which devices you can add, use the **add devices ?** command.

When adding interfaces with more than one port, add one port at a time. Use the **add device** command twice to add both ports of a dual-port adapter.

user *user_name*

Gives a user access to the device. You can authorize up to 50 users to access the device. Each *user_name* is eight characters and is case-sensitive.

When the first user is added, console login is automatically enabled. Each user added must be assigned one of the permission levels defined in Table 6.

When users are added, set login authentication to local. Otherwise a remote server must be used.

Table 6. Access Permission

Permission Level	Description
Administrator (A)	Displays configuration and user information, adds/modifies/deletes configuration and user information. The Administrator can access any router function.
Operator (O)	Views router configuration, views statistics, runs potentially disruptive tests, dynamically changes router operation, and restarts the router. Operators cannot modify the permanent router configuration. All actions can be undone with a system restart.
Monitor (M)	Views router configuration and statistics but cannot modify or disrupt the operation of the router.
Tech Support	Allows your service representative to gain access to the router if a password is forgotten. Cannot be assigned to users.

Note: To add a user, you must have administrative permission. You do not have to reinitialize the router after adding a user.

Example:

```
add user John
Enter password:
Enter password again:
Enter permission (A)dmin, (O)perations, (M)onitor [A]?
Do you want to add Technical Support access? (Yes or [No]):
```

Enter password

Specifies the access password for the user. Limited to 80 alphanumeric characters and is case-sensitive.

Enter password again

Confirms the access password for the user.

Enter permission

Specifies the permission level for the user: A, O, or M (see Table 6).

Boot

Use the **boot** command to enter the Boot CONFIG command environment. For Boot CONFIG information, see “Chapter 9. Using BOOT Config to Perform Change Management” on page 113.

Syntax:

boot

Change

Use the **change** command to modify an interface in the configuration,change your own password, or change user information.

Syntax:

change device . . .

user

Example:

```
change device
Which configured slot would you like to change? (1, 2) [1]? 2
Which slot would you like to change to? (1-2)  [1]? 1
Changed slot 2 to slot 1 in 1 intf (port) record...
```

device *device_type*

With the **change device** command you can:

- Change the slot of an existing interface. (Change slot x in interface record n to y where slot y is unoccupied.)
- Swap slots of two existing interfaces. (Swap slot x and slot y in interface records with x or y.)
- Replace the slot in an existing interface with the slot in another. (Interface configuration for slot x will become interface configuration for slot y. Interface records for slot y will be deleted.)

When the target slot is occupied:

1. If you select the “swap” option, the source and target slots are swapped in the interface records in which they appear.
2. If you select the “replace” option is selected, the interface configuration for slot x will become the interface configuration for slot y. Interface records for slot y will be deleted.

Example - Change slot 2 on interface 0 to unoccupied slot 1:

```
Config>list dev
Ifc 0 CHARM ATM                      Slot: 2  Port: 1

Config>change device
Which configured slot would you like to change? (2) [2]? 2
Which slot would you like to change to? (1-2)  [1]? 1

Changed slot 2 to slot 1 in 1 intf (port) record...

Config>list dev
Ifc 0 CHARM ATM                      Slot: 1  Port: 1
```

Example - Change (swap) slot 2 on interface 1 to occupied slot 1:

```
Config>list dev
Ifc 0 CHARM ATM                      Slot: 1  Port: 1
Ifc 1 CHARM ATM                      Slot: 2  Port: 1

Config>change device
Which configured slot would you like to change? (1, 2) [2]? 2
Which slot would you like to change to? (1-2)  [1]? 1

Configuration for slot 1 already exists. You can:
a - abort this operation
r - replace configuration
    (Interface configuration for slot 2 will become interface
     configuration for slot 1.  Interface records for slot 1
```

```
     will be deleted!)
s - swap configuration (slot 1 will be swapped with slot 2.)
s

Swapped slot 2 with slot 1 in 1 port record...

Config>list dev
Ifc 0 CHARM ATM                      Slot: 2  Port: 1
Ifc 1 CHARM ATM                      Slot: 1  Port: 1
```

Example - Change (replace) slot 1 on interface 1 to occupied slot 2:

```
Config>list dev
Ifc 0 CHARM ATM                      Slot: 2  Port: 1
Ifc 1 CHARM ATM                      Slot: 1  Port: 1

Config>change device
Which configured slot would you like to change? (1, 2) [2]? 1
Which slot would you like to change to? (1-2)  [1]? 2

Configuration for slot 2 already exists. You can:
a - abort this operation
r - replace configuration
    (Interface configuration for slot 1 will become interface
     configuration for slot 2.  Interface records for slot 2
     will be deleted!)
s - swap configuration (slot 1 will be swapped with slot 2.)
r

Moved slot 2 to slot 1 in 1 intf (port) record...

Config>list dev
Ifc 0 CHARM ATM                      Slot: 2  Port: 1
```

user Modifies the user information that was previously configured with the **add user** command.

Note: To change a user, you must have administrative permission.

Example:

```
change user
User name: []
Change password? (Yes or No)
Change permission? (Yes or [No])
```

Clear

Use the **clear** command to delete the router's configuration information from nonvolatile configuration memory.

Attention: Use this command only after calling your service representative.

Syntax:

clear

- all
- ap2 (AppleTalk 2)
- arp (ARP)
- asrt (Adaptive Source Route Protocol)
- appn (Advanced Peer-to-Peer Networking)
- atm (Asynchronous Transfer Mode)
- bgp (Border Gateway Protocol)
- boot
- device
- dn (DECnet)

els (Event Logging System Information)

hostname

ip (IP)

ipx (Novell IPX)

lnm

mcf

named-profiles

ospf (OSPF routing protocol)

prompt

snmp

srly (SDLC Relay)

tcp/ip-host

time (Time of day information)

user

vines (Banyan VINES)

To clear a process from nonvolatile configuration memory, enter the **clear** command and the process name. To clear all information from configuration memory, except for device information, use the **clear all** command. To clear all information, including the device information, use the **clear all** command and then the **clear device** command.

The **clear user** command clears all user information except the router console login information. This is left as enabled (if it was configured as enabled) even though the default value is “disabled”.

Notes:

1. To clear user information, you must have administrative permission.
2. There may be other items in the list, depending upon what is included in the software load.

Example: `clear els`

```
You are about to clear all Event Logging configuration information
Are you sure you want to do this (Yes or No):
```

Note: The previous message appears for any parameter configuration you are clearing.

Delete

Use the **delete** command to remove an interface from the list of devices stored in the configuration, or to remove a user. To use the **delete** command, you must have administrative permission.

Syntax:

delete interface . . .

dump-files

user . . .

dump-files
Deletes all of the system dump files from the hard drive .

Note: If you enter this command and a hard drive is not available, you will receive a message indicating that the drive is unavailable.

Example:

```
Config> delete dump-files
Number of existing dump files: 3
Are you sure you want to delete the dump files ? (Yes, No): [No] Yes
Dump files deleted.
```

interface [*intfc#***]**
To delete an interface, enter the interface or network number as part of the command. (Only devices that were added with the **add device** command can be deleted.) To obtain the interface number that the router assigns, use the **list device** command.

The delete interface command deletes the device configuration and any protocol information for that interface. However, the router will continue to run the previous configuration until it is .

If deleting a base ISDN interface or a base ATM interface, all virtual interfaces running on that base net will also be deleted. So, any dial circuits configured on a base ISDN interface will be removed when the ISDN interface is deleted. Also, when deleting an ATM base net, all LAN Emulation Clients running on the base ATM interface will be deleted.

user *user_name*
Removes user access to the router for the specified user.

Disable

Use the **disable** command to disable command completion, login from a remote console, system memory dumping, rebooting, or a specified interface.

Syntax:

disable command-completion
console-login
dump-memory . . .
interface . . .
reboot-system . . .

command-completion

Use the **disable command-completion** command to disable the automatic command completion function. See “Command Completion” on page 20 for a discussion of the automatic command completion function.

console-login
Disables the user from being prompted for a user ID and password on the physical console. The default is disabled.

interface *interface#*
Causes the specified interface to be disabled after issuing the **reload** command. The default is enabled.

dump-memory
Disables the dumping of system memory to the installed hard disk when a serious error occurs.

reboot-system
Disables the rebooting of the system when a serious error occurs. This may be desirable if the network service personnel wish to troubleshoot the error on-line. System rebooting cannot be disabled unless memory dumping is also disabled. If you attempt to disable system rebooting while memory dumping is enabled, system rebooting is aborted and the following message is displayed:

```
System reboot not disabled:  memory dumping must be disabled first
```

Enable

Use the **enable** command to enable command completion, login from a remote console, system memory dumping, rebooting, or a specified interface.

Syntax:

enable
- command-completion
- console-login
- dump-memory . . .
- interface . . .
- reboot-system . . .

command-completion

Use the **enable command-completion** command to enable the automatic command completion function, which assists with the command syntax. See “Command Completion” on page 20 for a discussion of the automatic command completion function.

console-login
Enables the user to be prompted for a user ID and password on the physical console. This is useful for security situations. If you do not configure any administrative users and you enable this feature, the following message appears:

```
Warning: Console login is disabled until an
administrative user is added.
```

Attention: Before enabling console login, save the configuration with console login disabled. If login authentication is set to a remote server using Radius or Tacacs+ and the router is unable to reach the authentication server, then access to the router is denied. By disabling the console login, a lock-out situation is prevented.

dump-memory
Enables the dumping of system memory to the installed hard disk if a serious error occurs. This may be desirable so that the state of the unit at the time of the error can be preserved for troubleshooting later. The dump memory function cannot be enabled unless system rebooting is enabled. If you attempt to enable the dump memory function while system rebooting is disabled, the dump memory function is not enabled and the following message is displayed:

```
System memory dump function not enabled:  rebooting must be enabled first
```

If you configured system dumping to save the first 3 dump files and 3 dump files already exist on the hard drive, the system displays the following message when you enable dump memory:

```
*** System dump cannot be enabled until the    ***
*** existing dump files are deleted.           ***
```

See the **set dump enable-mode** and **set dump save-mode** commands.

Example:

```
Config> enable dump

Current System Dump Status:
   System dump is currently disabled.
   Number of existing dump files:  0

Enable system memory dumping? [No]: Yes

Current System Dump Status:
   System dump is currently enabled.
   Number of existing dump files:  0
```

Note: If you enter this command and a hard drive is not available, you will receive a message indicating that the drive is unavailable.

interface *interface#*
Causes the interface to be enabled after issuing the **reload** command.

modem-control [carrier-wait or ring-wait] [service1 or service2]
Sets up the router for login on the physical console, if the physical console is connected to the router through a modem. Before using this command, be sure to:

- Set your modem for auto-answer.
- Verify that the console baud rate is equal to the modem baud rate.
- Verify that the cable connecting the modem to the router is configured correctly.
- Turn echo off by using the ATE0 command.
- Run in quiet mode by using the ATQ1 command.
- Verify that any necessary jumpers are set. Refer to your router's *User's Guide* more information.

The router automatically hangs up the modem when you log out. Also, if your modem becomes disconnected from the router while you are using it, the router logs you out.

Specify the service port for both the **enable modem-control carrier-wait** and the **enable modem-control ring-wait** commands. For routers with two service ports, also specify to which service port you connected the modem, either **service1** or **service2**. To enable *both* service ports, enable them separately.

Note: No console connection can be made with the router after enabling modem control unless you clear all configuration and restart the router.

You can tell the router to wait for the carrier-detect signal from the modem before sending Request to Send. This is the standard method of modem control.

You can tell the router to wait for the ring-indication signal before raising Request to Send or Data Terminal Ready. This is provided for countries requiring an earlier handshake.

Example:

```
Config> enable modem-control carrier-wait service1
```

reboot-system
Enables the rebooting of the system when a serious error occurs.

Event

Use the **event** command to enter the Event Logging System (ELS) environment so that you can define the messages that will appear on the console. Refer to "Chapter 13. Using the Event Logging System (ELS)" on page 145 for information about ELS.

Syntax:

event

Feature

Use the **feature** command to access configuration commands for specific router features outside of the protocol and network interface configuration processes.

Syntax:

feature [*feature#* or *feature-short-name*]

All IBM 8210 features have commands that are executed by:

- Accessing the configuration process to initially configure and enable the feature, as well as perform later configuration changes.
- Accessing the console process to monitor information about each feature, or make temporary configuration changes.

The procedure for accessing these processes is the same for all features. The following information describes the procedure.

Enter a question mark after the **feature** command to obtain a listing of the features available for your software release.

To access a feature's configuration prompt, enter the **feature** command followed by the feature number or short name. Table 7 lists available feature numbers and names.

Table 7. IBM 8210 Feature Numbers and Names

Feature Number	Feature Short Name	Accesses the following feature configuration process
2	MCF	MAC Filtering
6	QoS	Quality of Service

Once you access the configuration prompt for a feature, you can begin entering specific configuration commands for the feature. To return to the CONFIG prompt, enter the **exit** command at the feature's configuration prompt.

List

Use the **list** command to display configuration information for all network interfaces, or configuration information for the router.

Syntax:

list configuration
devices
named-profile
patches . . .
users . . .
vpd

configuration
Displays configuration information about the router.

Example: `list configuration`

```
Hostname: acctg
Maximum packet size: [autoconfigured]
Maximum number of global buffers: [autoconfigured]
Number of spare interfaces: 0
Console baudrate:  9600 (Autobaud)
Console inactivity timer (minutes): 0
Physical console login: disabled
Modem Control Enabled, using CARRIER-WAIT type control
System rebooting on error: disabled
System memory dumping: disabled
Contact person for this node: [none]
Location of this node: [none]

Configurable Protocols:
Num Name  Protocol
0   IP    DOD-IP
3   ARP   Address Resolution
7   IPX   NetWare IPX
11  SNMP  Simple Network Management Protocol
10  BGP   Border Gateway Protocol
12  OSPF  Open SPF-Based Routing Protocol
23  ASRT  Adaptive Source Routing Transparent Enhanced Bridge
24  HST   TCP/IP Host Services

Configurable Features:
Num Name  Feature
2   MCF   MAC Filtering
6   QoS   Quality of Service

27616 bytes of configuration memory free
```

devices
Displays the relationship between an interface number and the hardware interface. You can also use this command to check that a device was added correctly issuing the **add** command.

Example: `list devices`

```
Ifc 0 CHARM ATM Adapter      Slot: 1  Port: 1
```

patches
Displays the values of patch variables that have been entered using the **patch** command.

Example:

```
list patches
Patched variable            Value

mosheap-lowmark             20
```

vpd Displays the hardware and software vital product data.

Load

Use the **load** command to list, add, or delete optional software packages (for example, APPN).

Syntax:

load	add package *packagename*
	delete package *packagename*
	list . . .

The software is divided into multiple load modules. These load modules are grouped into software packages. Some of these software packages are optional because, although they are shipped with the product, they are not automatically loaded.

To load and run optional software packages:

1. Add the package using the **load add** command.
2. Reboot. This action loads the optional software into the device's memory.
3. Configure the optional software.
4. Save the configuration.
5. Reboot the device. This action enables the software with the new configuration.

add package *packagename*
: Adds a software package to the software. The *packagename* is the name of the package of load modules you want to include in the software.

delete package *packagename*
: Removes a software package from the software. The *packagename* is the name of the package of load modules you want to remove from the software.

list
: Lists either the packages in the software load that are available but not configured, or the packages that are configured in the software load. You can specify one of the following:

  available
  : Lists the software packages in the current software load that are not configured.

  configured
  : Lists the software packages in the current software load that are configured.

Network

Use the **network** command to enter the network interface configuration environment for supported networks. Enter the interface or network number as part of the command. (To obtain the interface number, use the CONFIG **list device** command.) The appropriate configuration prompt (for example, `TKR Config>`) will be displayed. See the network interface configuration chapters in this book for complete information on configuring your types of network interfaces.

Syntax:

network	*interface#*

Notes:

1. If you change a user-configurable parameter, you may use the GWCON **reset interface** command, or you may **reload** the router for the change to take effect. To do so, enter the **reload** command at the OPCON prompt (*).
2. Not all network interfaces are user-configurable. For interfaces that you cannot configure, you receive the message: `That network is not configurable.`

Patch

Use the **patch** command for modifying the router's global configuration. Patch variables are recorded in nonvolatile configuration memory and take effect immediately; you do not have to wait for the next restart of the router. This command should be used only for handling uncommon configurations. Anything that you commonly configure should still be handled by using the specific configuration commands. The following is a list of the current patch variables documented and supported for this release.

Syntax:

patch

- bgp-subnets
- ip-default-ttl
- ip-mtu
- more-lines
- mosheap-lowmark
- ospf-import-rate
- ping-size
- ping-ttl
- rip-static-suppress

bgp-subnets *new value*
If you want the BGP speaker to advertise subnet routes to its neighbors, set *new value* to 1. The default is 0.

dls-ignore-lfs *new value*
When set to 1, DLSw ignores the "largest frame" size bits in source-routed frames when setting up a circuit. This avoids circuit setup problems with some older LAN products that do not set these bits correctly. The default is 0.

ip-default-ttl *#_of_packets*
The TTL used in packets that are originated by the router. The default is 64.

Note: It is preferable to set this parameter with the **set ttl** IP configuration command. (See the "Set" section of the "Using and Configuring IP" chapter of *Multiprotocol Switched Services (MSS) Interface Configuration and Software User's Guide* .) This patch variable remains for compatibility with configurations from older releases.

ip-mtu *bytes*
This parameter limits the IP MTU size to the specified value. When this parameter is set, the IP MTU size on a given network interface is set to the lesser of the ip-mtu value and the largest value that network interface's configured frame size can accommodate.

more-lines *#_of_lines*
The number of lines to display on the console when listing long output.

mosheap-lowmark *new value*
This parameter specifies the percentage of free MOS heap memory, at which the device notifies the operator that an out-of-memory error is imminent. This notification allows the operator to take action to free up MOS heap memory before the device receives an error and stops.

When the operator receives notification, the operator can reconfigure the router and then reboot, minimizing the outage to the network. Specifying 0 for this parameter suppresses this warning.

Valid Values: 0 to 100

Default Value: 10

ospf-import-rate *rate*
Number of routes imported per second.

ping-size *bytes*
The size of the data portion (that is, excluding IP and ICMP headers) of the ICMP PING packet that is sent via the `IP>`**ping** command. Default: 56 bytes. (The size of the PING data can also be entered as a parameter of the **ping** command as described in the "Ping" section of the "Monitoring IP" chapter of *Multiprotocol Switched Services (MSS) Interface Configuration and Software User's Guide* .)

ping-ttl *seconds*
The TTL (time-to-live) sent in PINGs by the `IP>`**ping** command. Default: 64. (The TTL can also be entered as a parameter of the **ping** command as described in the "Ping" section of the "Monitoring IP" chapter of *Multiprotocol Switched Services (MSS) Interface Configuration and Software User's Guide*.

rip-static-suppress *new value*
When set to a non-zero value, static routes will not be advertised by RIP over a given interface unless the `IP config>` **enable send static** command is given for the interface. This changes the semantics of the **enable send static** command. When rip-static-suppress is equal to 0 (the default), the list of the routes advertised via RIP is the union of those specified by the interface's RIP flags.

Note: You must specify the complete name of the patch variable that you want to change. You cannot use an abbreviated syntax for the patch name.

Performance

Use the **performance** command at the `Config>` prompt to enter the configuration environment for performance. See "Chapter 15. Configuring and Monitoring Performance" on page 213 for more information.

performance

Protocol

Use the **protocol** command at the `Config>` prompt to enter the configuration environment for the protocol software installed in the router.

Syntax:

protocol [*prot#* or *prot_name*]

The **protocol** command followed by the desired protocol number *or* short name lets you enter a protocol's command environment. After you enter this command, the prompt of the specified protocol appears. From the prompt, you can enter commands specific to that protocol. To return to `Config>`, enter the **exit** command.

Notes:

1. To see the names and numbers of the protocols in your software load, at the `Config>` prompt, enter **list configuration**.
2. When you change a user-configurable parameter, you may be able to use the protocol's GWCON **reset** command, or you may have to restart the router for the change to take effect. To do so, enter the **reload** command at the OPCON prompt (*).

   The changes you make through CONFIG are kept in a configuration database in nonvolatile memory and are recalled when you restart the router.

Qconfig

Use the **qconfig** command to initiate Quick Config. Quick Config allows you to configure parameters for bridging and routing protocols without entering separate configuration environments.

Syntax:

qconfig

Note: For complete information on using the Quick Config software provided with your router, see "Appendix A. Quick Configuration Reference" on page 495.

Set

Use the **set** command to configure various system-wide parameters.

Syntax:

set
- contact-person . . .
- down-notify . . .
- dump enable-mode
- dump save-mode
- global-buffers
- hostname
- inactivity-timer
- input-low-water
- location . . .
- logging level
- packet-size
- prompt
- receive-buffers

spare-interfaces

contact-person *sysContact*

Sets the name or identification of the contact person for this managed SNMP node. There is a limit of 80 characters for the *sysContact* name length.

This variable is for information purposes only and has no effect on router operation. It is useful for SNMP management identification of the system.

down-notify *interface# # of seconds*

Allows the user to specify the number of seconds before declaring an interface as being down. The normal maintenance packet interval is 3 seconds, and it takes four maintenance failures to declare the interface as down.

The **set down-notify** command is used primarily when tunneling LLC traffic over an IP network using OSPF. If an interface goes down, OSPF cannot detect it fast enough because of the length of time that it takes for an interface to be declared down. Therefore, LLC sessions would begin to timeout. You can set the down-notify timer to a lower value, allowing OSPF to sense that an interface is down quicker. This enables an alternate route to be chosen more quickly, which will prevent the LLC sessions from timing out.

Note: If the **set down-notify** command is executed on one end of a serial link, the same command must be performed at the other end of the link or the link may not come up and stay up.

Interface#

The number of the interface you are configuring.

# of seconds

The down notification time value that specifies the maximum time that will elapse before a down interface is marked as such. Large values will cause the router to ignore transient connection problems, and smaller values will cause the router to react more quickly. The range of values is 1 to 300 seconds and the default is 0, which sets the 3-second period. Setting the down notification time to 0 will restore the default time for that interface.

The **list devices** command will show the down notification time setting for any interface that has the default value overridden.

dump enable-mode

Specifies whether dumping is enabled following the next system dump. If you configure the save mode (see the **set dump save-mode** command) to save the first three dumps and the system has already created the third dump file, dumping is disabled regardless of your specification. At the time the system creates the third dump file, you will receive the following message:

```
Active Dump Detected.
Dump Compression in Progress, please be patient ...

*** System dumping is being DISABLED because dumping is ***
*** configured to save the 3 initial dumps, but 3       ***
*** dump files already exist.                           ***
```

Example:

```
Config> set dump enable-mode

Current System Dump Settings:
   Disable System Dump following the next system dump.
   Save the last 3 (most recent) dump files.

Do you want to change system dump enable-mode to
re-enable System Dump following the next system dump ? (Yes, No): [No] Yes

Current System Dump Settings:
   Re-enable System Dump following the next system dump.
   Save the last 3 (most recent) dump files.

Current System Dump Status:
   System dump is currently enabled.
   Number of existing dump files:  2
```

Default value: disable

Note: Dumping is enabled with the **enable dump-memory** command.

dump save-mode

Specifies whether to save the first three (initial) system dump files or the last three (most recent). See the **dump enable-mode** for a consideration for using recent mode as opposed to initial mode.

Example:

```
Config> set dump save-mode

Current System Dump Settings:
   Re-enable System Dump following the next system dump.
   Save the last 3 (most recent) dump files.

Do you want to change system dump save-mode to
save the first (initial) dump files ? (Yes, No): [No] Yes

Current System Dump Settings:
   Re-enable System Dump following the next system dump.
   Save the first 3 (initial) dump files, then disable system dump.

Current System Dump Status:
   System dump is currently enabled.
   Number of existing dump files:  2
```

Default value: recent

global-buffers *max#*

Sets the maximum number of global packet buffers, which are the packet buffers used for locally originated packets. The default is to autoconfigure for the maximum number of buffers (up to 1000). To restore the default, set the value to 0. To display the setting for global-buffers, use the **list configuration** command.

hostname *name*

Adds or changes the router name. The router name is for identification only; it does not affect any router addresses. The *name* must be less than 78 characters and is case sensitive.

inactivity-timer *#_of_min*

Changes the setting of the Inactivity Timer. The Inactivity Timer logs out a user if the remote or physical console is inactive for the period of time specified in this command. This command affects only consoles that require login. The default setting of 0 turns the inactivity timer off, indicating that no logoff is performed, no matter how long a console remains inactive.

input-low-water *interface# low_ #_of_receive_buffers*

Allows you to configure the value of the low number of receive buffers, or packets, on a per-interface basis, thus overriding the default values.

The memory allocation strategy changes to conserve buffers when the number of free buffers is equal to or less than the low or low-water mark value. When a packet is received, and the current value of the interface is less than the low water value, then that packet is eligible for flow control (dropping).

The range of values is 1 to 255. The default is both platform and device specific. Setting the value to 0 restores the autoconfigured default.

Interface# is the number of the interface you are configuring.
Low_#_of_receive_buffers is the low water value.

Lowering the value will make it less likely that packets from this interface will be dropped when sent on congested networks. However, lowering the value may negatively affect performance if it drops packets to the extent that the receive queue is frequently empty. Raising the value has the opposite effect.

Type the **QUEUE** or **BUFFER** command at the GWCON prompt (**+**) to show the low setting.

location *sysLocation*

Sets the physical location of an SNMP node. There is a limit of 80 characters for the *sysLocation* name length. This variable is for information purposes only and has no effect on router operation. It is useful for SNMP management identification of the system.

logging level *#*

Controls the output of messages that have not yet been converted to the ELS. (Refer to for more information about the ELS.) The logging level is recorded in the configuration. When the router is powered on or restarted, the logging level takes effect and determines message output. The default logging level is 76. Logging level 0 equates to no logging level.

```
Example: set logging level 76
```

packet-size *max_packet_size_in_bytes*

Establishes or changes the maximum size for global buffers and receive buffers. If you specify a value of 0 as the maximum packet size, the size of receive buffers for an interface is based on that interface's configured packet size and the packet size of global buffers are autoconfigured. If you specify a non-zero value, the configured value is used as the global buffer packet size and any interfaces that have a configured packet size that is larger than the maximum packet size will use the maximum packet size for their receive buffers. A value of 0 (for autoconfigure) is the default.

Attention: Use this command only under direct instructions from your service representative. ***Never*** use it to reduce packet size – ***only*** to increase it.

prompt *user-defined-name*

Adds a user-defined name as a prefix to all operator prompts, replacing the hostname.

The user-defined-name can be any combination of characters, numbers, and spaces up to 80 characters. Special characters may be used to request additional functions as described in Table 8 on page 110.

Example:

```
set prompt
What is the new MOS prompt [y]? AnyHost 99
AnyHost 99 Config>
```

Table 8. Additional Functions Provided by the Set Prompt Level Command

Special Characters	Function Provided by the Set Prompt Level Command

$n	Displays the hostname. This is useful when you want the hostname included in the prompt. For example:
	`Config> set prompt`
	`What is the new MOS prompt [y]? $n`
	`hostname:: Config>`

$t	Displays the time. For example:
	`Config> set prompt.`
	`What is the new MOS prompt [y]? $t`
	`02:51:08[GMT-300] Config>`

$d	Displays the current date-month-year. For example:
	`Config> set prompt.`
	`What is the new MOS prompt [y]? $d`
	`26-Feb-1997 Config>`

$v	Displays the software VPD information in the following format: `program-product-name Feature xxxx Vx.x PTFx RPQx`
$e	Erases one character *after* this combination within the user-defined prompt.
$h	Erases one character *before* this combination within the user-defined prompt.
$_	Adds a carriage return to the user-defined prompt.
$$	Displays the $.

Note: You can combine these commands. For example:
`Config> set prompt`
`What is the new MOS prompt [y]? $n::$d`
`hostname::26-Feb-1997 Config>`	

receive-buffers *interface# max#*

Adjusts the number of private receive buffers for most interfaces.

The range is 5 to 1000.

Table 9. Default and Maximum Settings for Interfaces

Interface	Default	Maximum
ATM	80	1000
TKR	40	250
FDDI	80	80

spare-interfaces ***n***

Defines ***n***, the number of spare interfaces, for this device. See “Configuring Spare Interfaces” on page 88 for additional information.

System Retrieve

Use the **system retrieve** command to retrieve one or more memory image files from the installed hard drive after a serious error has occurred.

Syntax:

system retrieve

Uses TFTP to send selected memory image files to a remote host. The system will prompt you for the remote host's IP address and file names.

If there are no dump files, you will receive the following message:

```
No dump files exist to retrieve
```

System View

Use the **system view** command to display the current system dump settings and the status of the system dumps, including how many dump files exist. You can also display a summary of the dump files.

Syntax:

system view

Time

Use the **time** command to set the IBM 8210 system clock and date, and to display the values on the user console. These values can then be used to time-stamp ELS messages.

Note: The IBM 8210 has a hardware clock that maintains the date and time after router reinitialization.

Syntax:

time host . . .
list
offset
set . . .
sync . . .

host *IP_address*
Sets the IP address of the RFC 868-compliant host that will be used as the time source. This is the address of a host which will respond to an empty datagram on UDP port 37 with a datagram containing the current time.

list Displays all configured time-related parameters. This includes the current time (if set) and the source of the time (operator or IP address from which time was last received).

```
Example: time list
05:20:27  Wednesday December 7, 1994
Set by: operator
Time Host:  131.210.4.1
Sync Interval: 10 seconds GMT
Offset:  -300 minutes
```

offset *minutes*
Defines the time zone, in minutes, offset from GMT (Greenwich Mean Time). Note that values west of GMT are negative. For example, EST is 5 hours earlier than GMT, so the command would be **time offset -300**.

Valid values: -720 to 720

Default value: 0

set <*year month date hour minute second***>**
Prompts you to set the current time. If you do not specify the entire time in

the command, you are prompted for the remaining values. You can change the date as shown in the following example.

```
Example: time set
year [1996] 1997
month [12]?
date [6]? 7
hour [11]? 12
minute [3]?
second [2]?
```

sync *seconds*

Sets the period, in seconds, at which the router will poll the time host for the current time.

Unpatch

Use the **unpatch** command to restore the values of the patch variables entered with the **patch** command to their default values. See the **patch** command in “Patch” on page 104 for details.

Syntax:

unpatch *variable_name*

Note: You ***must*** specify the complete name of the patch variable to be restored.

Update

Use the **update** command to update the configuration memory when you receive a new software load.

Syntax:

update version-of-SRAM

Follow the instructions on the release notice sent with the software. The **update** command is the last command that you enter when loading new software. After you enter this command, the console displays a message indicating configuration memory is being updated.

Write

Use the **write** command to save a configuration to the device before reloading.

Syntax:

write

If you fail to issue the write command and try to reload the device, you will be asked if you want to save the configuration. The configuration is saved in the next CONFIG on the hard disk in the bank you are currently using.

Chapter 9. Using BOOT Config to Perform Change Management

This chapter describes how to use the Boot/Dump Configuration process. This chapter includes the following sections:

- "Understanding Change Management"
- "Using the Trivial File Transfer Protocol (TFTP)"
- "Loading an Image at a Specific Time" on page 114

Understanding Change Management

Change management is the handling of software and configuration data for an IBM 8210. This involves:

1. Moving code and configuration data to and from the IBM 8210
2.
3. Selecting and activating specific combinations of software and configuration.

The change management functions are available by entering the **boot** command at the `Boot config>` prompt (talk 6), or the firmware should the box be in a condition where the hard drive or compact flash does not contain viable software (that is, you cannot access talk 6).

The IBM 8210 code and configuration data storage resource is divided into areas called "system banks" (banks for short), each containing a single version of the operational code and any other files pertinent to that release of the code. Up to four configuration files are associated with each bank's software.

The general change management model of the IBM 8210 is to introduce new code and/or configuration data to the system while the system runs at its present level and then activate the changed code or configuration data set later. If for some reason the new code or configuration does not function as expected, you have the ability to revert to the previous version of the configuration.

Using the Trivial File Transfer Protocol (TFTP)

TFTP is a file transfer protocol that runs over the Internet UDP protocol. This implementation provides multiple, simultaneous TFTP file transfers between an IBM 8210's non-volatile configuration memory, image bank, and remote hosts.

TFTP allows you to:

- Get a configuration file from a server to an IBM 8210
- Put a configuration file from an IBM 8210 to a server

TFTP transfers involve a *client* node and a *server* node. The client node generates a TFTP Get or Put request onto the network. The IBM 8210 acts as a client node by generating TFTP requests from the IBM 8210 console using the `Boot config>` process **tftp** command.

The client can transfer a copy of a configuration file or image file stored in the image bank of a server.

© Copyright IBM Corp. 1996, 1998

Using BOOT Config

The server is any device (for example, a personal computer or workstation) that receives and services the TFTP requests. Use the ELS subsystem TFTP message log to view the transfer in progress.

Loading an Image at a Specific Time

There may be occasions when you may want to load a device on a specific day and time when you will be unavailable. You can configure the device to perform a timed load using the **timedload activate** command. Other commands allow you to view a device's scheduled load information or cancel a scheduled load. See "Change Management Configuration Commands" on page 115 for information on these commands.

Chapter 10. Configuring Change Management

This chapter describe the Change management configuration commands. It includes the following sections:

- "Accessing the Change Management Configuration Environment"
- "Change Management Configuration Commands"

Accessing the Change Management Configuration Environment

To enter the change management configuration command environment, use the CONFIG **boot** command. When the router's software is initially loaded, it is running in the OPCON process, signified by the * prompt. From the * prompt:

1. Enter **talk 6**.
2. At the `Config>` prompt, type **boot**.

To return to the CONFIG process, type **exit**.

Change Management Configuration Commands

This section describes the Change Management Configuration commands. Each command includes a description, syntax requirements, and an example. Table 10 summarizes the Change Management Configuration commands.

After accessing the Change Management Configuration environment, enter the configuration commands at the `Boot config>` prompt.

Table 10. Change Management Configuration Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Add	Adds an optional description to a configuration file.
Copy	Copies boot files and configuration files to or from banks.
Describe	Displays information about the stored loadfile images.
Disable	Turns off various change management functions.
Enable	Turns on various change management functions.
Erase	Erases a stored image or a configuration file.
List	Displays information about configuration files and scheduled load information.
Lock	Prevents the device from overwriting the selected configuration with any other configuration.
Set	Selects code bank and configuration to be used.
TFTP	Initiates TFTP file transfers between the IBM 8210 and remote servers.
Timedload	Schedules a load into the device on a specific day and time, cancels a scheduled load, or displays scheduled load information.
Unlock	Removes the lock from a configuration allowing the configuration to be updated by the device.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

© Copyright IBM Corp. 1996, 1998

Add

Use the **add** command to add an optional description to a configuration file.

Syntax:

add configuration *file description*

load *image description*

Example: Boot config> **add**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 01:39 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 01:52 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:30 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:30 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:24 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (A, B, F): [A]
Select the source configuration:  (1, 2, 3, 4): [1] 3
Enter the description of the file: () New config for today

Attempting to set description for bank A configuration 3.

Operation completed successfully.


Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:58 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        | New config for today            | 09 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 01:05 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:24 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

  Auto-boot mode is enabled. Fast-boot mode is disabled.
```

Copy

Use the **copy** command to copy configuration files and load images to and from banks.

Syntax:

copy configuration *file*

load *image*

Example: Boot config>**copy load**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 01:39 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 01:52 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:37 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:37 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (A, B, F): [A] b
Select the destination bank:  (A, B): [B] a
Copy SW load image from: bank B
                     to: bank A.


Operation completed successfully.
```

Example: Boot config>**copy configuration**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - CORRUPT        |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 01:39 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 01:52 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:37 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:37 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:24 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (A, B, F): [A]
Select the source configuration:  (1, 2, 3, 4): [1]
Select the destination bank:  (A, B, F): [B]

Select the destination configuration:  (1, 2, 3, 4): [1]
Copy SW configuration from: bank A, configuration 1
                       to: bank B, configuration 1.
/hd0/sys0/CONFIG0 --> /hd0/sys1/CONFIG0

Operation completed successfully.
```

If the copy fails you may receive one of the following messages:

Error: Active bank cannot be overwritten or erased.
You attempted to copy a configuration into the bank currently in use by the IBM 8210.

Error: File copy failed.
This condition occurs when the copy operation fails for reasons other than copying to the active configuration. The most common cause is specifying the same source and destination configurations. When you list (see “List” on page 121) the configurations, CORRUPT appears next to the bank that is damaged.

Describe

Use the **describe** command to display information about a stored image.

Syntax: describe

Example: Boot config>**describe**

```
+-------------------------+-------------------------+-------------------------+
|         BANK A          |         BANK B          |          BANK F         |
| Product ID -   8210-MSS | Product ID -   8210-MSS | Product ID -   8210-MSS |
| Version   2.1           | Version   2.1           | Version   2.1           |
| Mod       0 PTF       0 | Mod       0 PTF       0 | Mod       0 PTF       0 |
| Feat.  8707 RPQ       0 | Feat.  8707 RPQ       0 | Feat.  8707 RPQ       0 |
| Date        31 Dec 1996 | Date        31 Dec 1996 | Date        31 Dec 1996 |
+-------------------------+-------------------------+-------------------------+
```

Disable

Use the **disable** command to turn off various change management functions.

Syntax:

disable auto-boot
fast-boot

auto-boot
Disabling auto-boot causes the router boot sequence to stop at the service recovery interface, without running the router operational code. The default auto-boot mode is “enabled”.

Example:

```
Boot config>disable auto-boot
Auto-boot mode is now disabled
```

fast-boot
Disabling fast-boot causes the router to run diagnostic tests when the router is booting during a power-on or a software reload. This provides better hardware error detection but results in slower boot times. This is the default mode, and is recommended whenever the router is in a production environment.

Enable

Use the **enable** command to turn on various change management functions.

Syntax:

enable auto-boot
fast-boot

auto-boot

Enabling auto-boot causes the router boot to the router operational code without stopping at the service recovery interface. The default auto-boot mode is “enabled”

Note: To enable auto-boot mode using this command, you must also have unattended mode selected in the firmware.

fast-boot

Enabling fast-boot causes the router to skip diagnostic tests when the router is booting during a power-on or a software reload. This reduces hardware error detection but results in faster boot times. The default mode is “disabled,” which is recommended whenever the router is in a production environment.

Example:

```
Boot config>enable fast-boot
Fast-boot mode is now enabled
```

Erase

Use the **erase** command to erase a stored image or a configuration file.

Syntax:

erase configuration [file]

load [image]

config or load

Erases a configuration file or a load image. Enter the config number to be erased after the **erase** command.

Example: `Boot config>erase load`

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - CORRUPT        |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:39 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:24 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the bank to erase:  (A, B, F): [A] a
Erase SW load image from bank A.

Operation completed successfully.


Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:58 |
```

```
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:39 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

  Auto-boot mode is enabled.  Fast-boot mode is disabled.
```

Example: Boot config>**erase configuration**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs           | 01 Jan 1970 01:13 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 01:26 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 01:39 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (A, B, F): [A]
Select the configuration to erase:  (1, 2, 3, 4): [1] 3
Erase SW configuration file from bank A, configuration 3.

Operation completed successfully.


Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                |                   |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:14 |
| CONFIG 2 - AVAIL   *   | test config for pubs           | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:26 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

  Auto-boot mode is enabled.  Fast-boot mode is disabled.
```

Notice that the list command displays **NONE** by bank A, config 3.

If the erasure fails, a message indicating the failure appears on the console with the banks that failed.

List

Use the **list** command to display information about which load images and configuration files are available and active. This command may also be used to display boot options and scheduled load information.

Syntax:

list

Example: Boot config>**list**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:39 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:24 |
+------------------------+---------------------------------+-----------------+
  * - Last Used Config      L - Config File is Locked
  Auto-boot mode is enabled.  Fast-boot mode is disabled.


 Time Activated Load Schedule Information...

The router is scheduled to reload as follows.

Date:  June 26, 1997
Time:  16:30
The load modules are in bank A.
The configuration is CONFIG 1 in bank A.
Boot config>
```

The possible file status descriptors are:

ACTIVE
: The file is currently loaded and is running on the 8210

AVAIL This is a valid file that can be made ACTIVE.

CORRUPT
: The file was damaged or not loaded into the 8210 completely. The file must be replaced.

LOCAL
: The file will be used only on the next reload or reset. After the file is used, it will be placed in AVAIL state.

PENDING
: This file will be loaded on the next reload, reset, or power-up of the 8210.

Lock

Use the **lock** command to prevent the device from overwriting the selected configuration with any other configuration.

Syntax:

lock

Example: Boot config>**lock**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970 01:03 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:26 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:24 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

Auto-boot mode is enabled.  Select the source bank:  (A, B, F): [A]
Select the source configuration:  (1, 2, 3, 4): [1] 4
Attempting to lock bank A and configuration 4.

Operation completed successfully.


Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:13 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL   L   |                                 | 01 Jan 1970 00:26 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 |                   |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 |                   |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:24 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

  Auto-boot mode is enabled.  Fast-boot mode is disabled.
```

Note: Note that bank A config 4 is marked with an “L.”

Set

Use the **set** command to select the code bank, the configuration to use, and the duration of use. The valid durations are:

once The configuration is active for the next boot only.

always
The configuration is active for all subsequent boots until changed again.

Syntax:

set

Example: Boot config>**set**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970 01:03 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:13 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:26 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:24 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (A, B, F): [A] b
Select the source configuration:  (1, 2, 3, 4): [1] 4
Select the duration to use for booting:  (once, always): [always]
Set SW to boot using bank B and configuration 4, always.

Operation completed successfully.


Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:13 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:26 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:24 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

   Auto-boot mode is enabled.  Fast-boot mode is disabled.
```

TFTP

Use the **tftp** command to initiate TFTP file transfers between the 8210 and remote servers.

Note: When you unzip an image, you will see multiple files ending in ".ld". Use the **tftp get load modules** command to get multiple load modules.

Syntax:

tftp get	config
	load modules
tftp put	config
	load single *image*

load modules

Example: Boot config>**tftp get load single**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970 01:03 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:01 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:14 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Specify the server IP address (dotted decimal): : [1.2.3.4] 192.9.200.1
Specify the remote file name: : (/u/bin) /usr/8210load/nce.img
Select the destination bank:  (A, B, F): [A] a
  TFTP SW load image
  get:   /usr/8210load/nce.img
  from:  192.9.200.1
  to:    bank A.

Operation completed successfully.
```

Note for Dynamic Loading of Software: All of the load modules in the specified directory will be retrieved as part of the load going into the bank. For loads for releases prior to Version 1, Release 2, this will be a single load module. For Version 1, Release 2 loads and later, this may be multiple load modules.

Example: Boot config>**tftp get load modules**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970 01:03 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:01 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:14 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Specify the server IP address (dotted decimal): : [1.2.3.4] 192.9.200.1
Specify the remote modules directory: : (/u/bin/) /usr/8210load/
Select the destination bank:  (A, B, F): [A] a
  TFTP SW load image
  get:   /usr/8210load/LML.ld
  from:  192.9.200.1
  to:    bank A.

Operation completed successfully.
```

Notes:
When putting files to a server:

1. Make sure that the files on the target server have the appropriate permissions that would allow anyone to write to those files. If not, the put operation will fail.
2. You must be aware of the files you are putting to the target server.To determine whether the image in the bank is a single module or multiple modules, use the **describe** command. A load prior to Version 1, Release 2 is a single module. Loads at Version 1, Release 2 or after are multiple modules.

Timedload

Use the **timedload** command to schedule a load on a device, cancel a scheduled load, or view scheduled load information.

This command allows you to load the device outside peak network traffic periods when support personnel may not be present.

Note: You may also use the Configuration Program to schedule a reload for a device, which is not affected by reloads or power outages. These circumstances would normally cause the reload to be lost. See the chapter "Using the Configuration Program" in *Configuration Program User's Guide* for details.

Syntax:

timedload activate
deactivate
view

activate
Schedules a load on the device. You will be prompted for information for a time-activated load similar to the **tftp get load** and **tftp get config** commands. See "TFTP" on page 123 for information about the parameters.

Time of day to load the device
Specifies the date and time to load the device. Specify the value as *YYYYMMDDHHMM*, where:

YYYY is the four-digit year

Note: If the current month on the device is December, the year data must be the current year or the following year. Otherwise, if the current month on the device is January through November, the year data must be the current year.

MM is the two digit month.

MM Valid Values: 01 to 12 with 01 representing January.

DD is the two-digit day of the month.

DD Valid Values: 01 to 31, depending on the value of MM.

HH is the two-digit hour in 24-hour time.

HH Valid Values: 00 to 23

MM is the two-digit minute of the hour.

MM Valid Values: 00 to 59

The following are examples of scheduling a load from different sources.

Example 1. Load modules and configuration source is a remote host:

```
Boot config>timedload activate

+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:39 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:24 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Time Activated Load Processing...

Select the bank to use:  (A, B): [A] a
Do you want to put load modules into the bank? (Yes, No, Quit): [Yes] yes

Do you want to retrieve a SINGLE image or a set of MODULES? [MODULES]? modules
 Specify the server IP address (dotted decimal): : [1.2.3.4] 192.9.200.1
Specify the remote modules directory: : (/u/bin) /usr/601bin/205img
The destination bank is bank A
TFTP SW load image
  get:   /usr/601bin/205img/
  from:  192.9.200.1
  to:    bank A.
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'

Operation completed successfully.

Do you want to put a configuration into the bank? (Yes, No, Quit): [Yes] yes

Specify the server IP address (dotted decimal): : [1.2.3.4] 192.9.200.1
Specify the remote file name: : (config.dat) /tftpboot/192.9.200.6.config
The destination bank is bank A
Select the destination configuration:  (1, 2, 3, 4): [1] 1
TFTP SW configuration file
  get:   /tftpboot/192.9.200.6.config
  from:  192.9.200.1
  to:    bank A, configuration 1.
tftp: connect to '192.9.200.1'

Operation completed successfully.

Time of day to load the router (YYYYMMDDHHMM) []? 199706261630
The load timer has been activated.
Boot config>
```

Example 2. Load modules and configuration source is a bank:

```
Boot config>timedload activate

+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:39 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
```

```
| IMAGE - ACTIVE         |                                  | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs             | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                  | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                  | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                  | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                  | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs             | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                  | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                  | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                  | 01 Jan 1970 00:24 |
+------------------------+----------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

Time Activated Load Processing...

Select the bank to use:  (A, B): [A] a
Do you want to put load modules into the bank? (Yes, No, Quit): [Yes] no

Do you want to put a configuration into the bank? (Yes, No, Quit): [Yes] no

Select the configuration to use:  (1, 2, 3, 4): [1] 1

Time of day to load the router (YYYYMMDDHHMM) []? 199706261630
The load timer has been activated.
Boot config>
```

deactivate

Cancels a scheduled load.

Example 1: Deactivate the time activated load

```
Boot config>timedload deactivate
Deactivate Load Timer Processing...

Do you want to deactivate the load timer? (Yes, No, Quit): [No] yes
The load timer has been deactivated.
Boot config>
```

view Displays scheduled load information.

```
Boot Config> timedload view
Time Activated Load Schedule Information...

The router is scheduled to reload as follows.

Date:  June 26, 1997
Time:  16:30
The load modules are in bank A.
The configuration is CONFIG 1 in bank A.
Boot config>
```

Unlock

Use the **unlock** command to allow the device to overwrite the selected configuration that was previously locked.

Syntax:

unlock

Example: Boot config>**unlock**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                  | 01 Jan 1970 01:03 |
| CONFIG 1 - AVAIL       | test config for pubs             | 01 Jan 1970 00:13 |
| CONFIG 2 - AVAIL   *   | test config for pubs             | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                  | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL    L  |                                  | 01 Jan 1970 00:26 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                  | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs             | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                  | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                  | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                  | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                  | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs             | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                  | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                  | 01 Jan 1970 00:14 |
```

```
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (A, B, F): [A]
Select the source configuration:  (1, 2, 3, 4): [1] 4
Attempting to unlock bank A and configuration 4.

Operation completed successfully.
Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                |                   |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:01 |
| CONFIG 2 - AVAIL   *   | test config for pubs           | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:14 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                | 01 Jan 1970 00:24 |
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

  Auto-boot mode is enabled.  Fast-boot mode is disabled.
```

Note: Note that bank A config 4 is no longer marked with an “L.”

Chapter 11. The Operating/Monitoring Process (GWCON - Talk 5) and Commands

This chapter describes the GWCON process and includes the following sections:

- "What is GWCON?"
- "Entering and Exiting GWCON"
- "GWCON Commands" on page 130

What is GWCON?

The Gateway Console (monitoring) process, GWCON (also referred to as CGWCON), is a second-level process of the router user interface.

Using GWCON commands, you can:

- List the protocols and interfaces currently configured in the router.
- Display memory and network statistics.
- Set current Event Logging System (ELS) parameters.
- Test a specified network interface.
- Communicate with third-level processes, including protocol environments.
- Enable and disable interfaces.

The GWCON command interface is made up of levels called modes. Each mode has its own prompt. For example, the prompt for the SNMP protocol is `SNMP>`.

If you want to know the process and mode you are communicating with, press **enter** to display the prompt. Some commands in this chapter, such as the **network** and **protocol** commands, allow you to access the various modes in GWCON.

Entering and Exiting GWCON

To enter GWCON from OPCON (*), choose one of the following methods:

1. Enter the OPCON **console** command:

   ```
   * console
   ```

2. At the OPCON prompt, enter the **status** command to find the PID of GWCON. (See page 9 for a sample output of the **status** command.)

   ```
   * status
   ```

   Then, enter the **talk** command followed by the PID number for GWCON:

   ```
   * talk 5
   ```

The console displays the GWCON prompt (+). If the prompt does not appear, press **enter**. Now, you can enter GWCON commands.

To return to OPCON, enter the OPCON intercept character. (The default is **Ctrl-P**.)

© Copyright IBM Corp. 1996, 1998

GWCON Commands

This section contains the GWCON commands. Each command includes a description, syntax requirements, and an example. The GWCON commands are summarized in Table 11.

To use the GWCON commands, access the GWCON process by entering **talk 5** and enter the GWCON commands at the (+) prompt.

Table 11. GWCON Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Activate	Enables a newly configured spare interface.
Buffer	Displays information about packet buffers assigned to each interface.
Clear	Clears network statistics.
Configuration	Lists status of the current protocols and interfaces.
Disable	Takes the specified interface off line.
Error	Displays error counts.
Event	Enters the Event Logging System environment.
Feature	Provides access to console commands for independent router features outside the usual protocol and network interface console processes.
Interface	Displays network hardware statistics or statistics for the specified interface.
Memory	Displays memory, buffer, and packet data.
Network	Enters the console environment of the specified network.
Performance	Provides a snapshot of the main processor utilization statistics.
Protocol	Enters the command environment of the specified protocol.
Queue	Displays buffer statistics for a specified interface.
Reset	Disables the specified interface and then re-enables it using new interface, protocol and feature configuration parameters.
Statistics	Displays statistics for a specified interface.
Test	Enables a disabled interface or tests the specified interface.
Uptime	Displays time statistics for the router.

Activate

Use the **activate** command to enable a spare interface on this device. See “Configuring Spare Interfaces” on page 88 for more information.

Syntax:

activate *interface#*

Buffer

Use the **buffer** command to display information about packet buffers assigned to each interface.

Note: Each buffer on a device is the same size and is dynamically built. Buffers vary in size from one device to another.

To display information about one interface only, enter the interface or network number as part of the command. To obtain the interface number, use the GWCON **configuration** command.

Syntax:

buffer [*network#* or]

Example:

```
buffer
               Input  Buffers:       Buffer sizes:
Nt  Interface  Req  Alloc  Low Curr  Hdr  Wrap  Data  Trail Total   Bytes Alloc


0   ATM/0       20    20     7    0  109   92    2052    7   2260   45200
```

Nt Network interface number associated with the software.

Interface
Type of interface.

Input Buffers:

Req Number of buffers requested.

Alloc Number of buffers allocated.

Low Low water mark (flow control).

Curr Current number of buffers on this device. The value will be 0 if the device is disabled. When a packet is received, if the value of *Curr* is below *Low*, then the packet is eligible for flow control. (See the **queue** command for conditions.)

Buffer Sizes:

Hdr Sum of the maximum hardware, MAC, and data link headers.

Wrap Allowance given for MAC, LLC, or Network layer headers due to protocol wrapping.

Data Maximum data link layer packet size.

Trail Sum of the largest MAC and hardware trailers.

Total Overall size of each packet buffer.

Bytes Alloc
Amount of buffer memory for this device. This value is determined by multiplying the values of *Alloc x Total*.

Clear

Use the **clear** command to delete statistical information about one or all of the router's network interfaces. This command is useful when tracking changes in large counters. Using this command does not save space or speed up the router.

Enter the interface (or net) number as part of the command. To get the interface number, use the GWCON **configuration** command.

Syntax:

clear *interface#*

Configuration

Use the **configuration** command to display information about the protocols and network interfaces. The output is displayed in three sections, the first section lists the router identification, software version, boot ROM version, and the state of the auto-boot switch. The second and third sections list the protocol and interface information.

Syntax:

configuration

Example:

```
configuration

Nways 8210 Multiprotocol Switching Server


Host name: [not configured]
Version: 2.0

Num Name  Protocol
0   IP    DOD-IP
3   ARP   Address Resolution
11  SNMP  Simple Network Management Protocol
12  OSPF  Open SPF-Based Routing Protocol
23  ASRT  Adaptive Source Routing Transparent Enhanced Bridge

Num Name  Feature
2   MCF   MAC Filtering
6   QOS   Quality of Service

1 Networks:
Net Interface  MAC/Data-Link         Hardware          State
0   ATM/0      ATM                   CHARM ATM         Up
```

- The first line gives the product name.
- The second line indicates whether a host name is configured.
- The third line lists the program/product number, Feature Number, Version, Release, PTF and RPQ information.
- The remaining lines list the configured protocols, followed by the configured features.

The following information is displayed for protocols:

Num Number that is associated with the protocol.

Name Abbreviated name of the protocol.

Protocol
Full name of the protocol.

The following information is displayed for features:

Num Number associated with the feature.

Name Abbreviated name of the feature.

Feature
Full name of the feature.

The following information is displayed for networks:

Net Network number that the software assigns to the interface. Networks are

numbered starting at 0. These numbers correspond to the interface numbers discussed under the CONFIG process.

Interface
Name of the interface and instance of this type of interface.

MAC/Data Link
Type of MAC/Data link configured for the interface.

Hardware
Specific kind of interface by hardware type.

State Current state of the network interface.

Testing
Indicates that the interface is undergoing a self-test. Occurs when the router is first started, when a problem is detected on the interface, or when the **test command** is used.

When an interface is operational, the interface periodically sends out maintenance packets and/or checks the physical state of the port or line to ensure that the interface is still functioning correctly. If the maintenance fails, the interface is declared down and a self-test is scheduled to run in 5 seconds. If a self-test fails, the interface transitions to the down state and the interval until the next self-test is increased up to a maximum of 2 minutes. If the self-test is successful, the network is declared up.

Up Indicates the interface is operational.

Down Indicates that the interface is not operational and has failed a self-test. The network will periodically transition to the testing state to determine if the interface can become operational again.

Disabled
Indicates that the interface is disabled. An interface can be disabled by the following methods:

- An interface can be configured as disabled using the CONFIG **disable** command. Each time the router is reinitialized, the interface's initial state will be disabled. It will remain in the disabled state until an action is taken to enable it.
- An interface can be disabled using the GWCON **disable** command. This method is temporary because the interface will revert to its configured state (enabled or disabled) when the router is reinitialized.
- The network manager can disable the interface through SNMP. This method is temporary because the interface will revert to its configured state (enabled or disabled) when the router is reinitialized.

When an interface is disabled, it remains disabled until one of the following methods is used to enable it:

- The GWCON **test** command is used to start a self-test of the interface.
- The network manager initiates a self-test of the interface through SNMP.

Not Present
Indicates that the interface's adapter is not plugged in.

Not Present is also used as the state for a null device. Spare interfaces are displayed as null devices until they are activated.

HW Mismatch
Indicates that the configured adapter type does not match the adapter type that is actually present in the slot.

Disable

Use the **disable** command to take a network interface off-line, making the interface unavailable. This command immediately disables the interface. You are not prompted to confirm, and no verification message displays. If you disable an interface with this command, it remains disabled until you use the GWCON **test** command or an OPCON **reload** command to enable it.

Enter the interface, or net number as part of the command. To obtain the interface number, use the GWCON **configuration** command.

Syntax:

disable *interface#*

Error

Use the **error** command to display error statistics for the network. This command provides a group of error counters.

Syntax:

error

Example:

```
error

                  Input   Input      Input      Input     Output  Output
Nt  Interface  Discards  Errors  Unk Proto  Flow Drop   Discards  Errors


0   ATM/0             0       0          0          0          0       0
```

Nt Network interface number associated with the software.

Interface
Type of interface.

Input Discards
Number of inbound packets which were discarded even though no errors were detected to prevent their being deliverable to a higher-layer protocol. The packets may have been discarded to free buffer space.

Input Errors
Number of packets that were found to be defective at the data link.

Input Unk Proto
Number of packets received for an unknown protocol.

Input Flow Drop
Number of packets received that are flow controlled on output.

Output Discards
Number of packets that the router chose to discard rather than transmit due to flow control.

Output Errors
Number of output errors, such as attempts to send over a network that is down or over a network that went down during transmission.

Note: The sum of the discarded output packets is not the same as input flow drops over all networks. Discarded output may indicate locally originated packets.

Event

Use the **event** command to access the Event Logging System (ELS) console environment. This environment is used to set up temporary message filters for troubleshooting purposes. All changes made in the ELS console environment will take effect immediately, but will go away when the router is reinitialized. See "Chapter 13. Using the Event Logging System (ELS)" on page 145 for information about the Event Logging System and its commands. Use the **exit** command to return to the GWCON process.

Syntax:

event

Feature

Use the **feature** command to access console commands for specific IBM 8210 features outside of the protocol and network interface console processes.

Enter a question mark after the **feature** command to obtain a listing of the features available for your software release.

To access that feature's console prompt, enter the **feature** command at the GWCON prompt followed by the feature number or short name. Table 7 on page 101 lists available feature numbers and names.

Once you access the prompt for that feature, you can begin entering specific commands to monitor that feature. To return to the GWCON prompt, enter the **exit** command at the feature's console prompt.

Syntax:

feature *feature#* or *feature-short-name*

Interface

Use the **interface** command to display statistical information about the network interfaces (for example, Ethernet). This command can be used without a qualifier to provide a summary of all the interfaces (shown in the following output) or with a qualifier to reveal detailed information about one specific interface.

Descriptions of detailed output for each type of interface are provided in the specific interface *Monitoring* chapters found in this guide. To obtain the interface number, use the GWCON **configuration** command.

Syntax:

interface [*interface#*]

Example: `interface`

```
                                        Self-Test  Self-Test  Maintenance
 Nt  Interface  Slot-Port  Port Name    Passed     Failed       Failed
 0   ATM/0         Slot:1     Port:1         1          0            0
```

Note: The display varies depending on the device.

Nt Global interface number.

Interface
Interface name.

Slot-Port
Slot number and port number of the interface.

Port Name
Port number, if applicable on the slot.

Self-Test Passed
Number of times self-test succeeded (state of interface changes from down to up).

Self-Test Failed
Number of times self-test failed (state of interface changes from up to down).

Maintenance Failed
Number of maintenance failures.

Memory

Use the **memory** command to display the current CPU memory usage in bytes, the number of buffers, and the packet sizes.

To use this command, free memory must be available. The number of free packet buffers may drop to zero, resulting in the loss of some incoming packets; however, this does not adversely affect router operations. The number of free buffers should remain constant when the router is idle. If it does not, contact your service representative.

Syntax:

memory

Example:

```
memory
Physical installed memory:        16 MB
Total routing (heap) memory:      12 MB
Routing memory in use:            13 %

                  Total  Reserve    Never     Perm     Temp     Prev
                                    Alloc    Alloc    Alloc    Alloc
Heap memory    12231155    26488 10687312  1438487   104924      432

Number of global buffers: Total = 300, Free = 300, Fair = 77, Low = 60
Global buff size: Data = 2048, Hdr = 17, Wrap = 72, Trail = 65, Total = 2208
```

Physical installed memory
The total amount of physical RAM installed in the router.

Total routing memory
The amount of memory available to the routing function, not including that allocated to the base operating system, system extensions, or options such as APPN. This is also called ″heap″ memory, and matches the ″Total″ heap memory size given in bytes shortly thereafter.

Routing memory in use
The percentage of total routing memory that is currently being used by the routing function. Heap memory currently in use is counted under the following headings **Perm Alloc** and **Temp Alloc**.

Heap memory:
Amount of memory used to dynamically allocate data structures.

Total Total amount of space available for allocation for memory.

Reserve
Minimum amount of memory needed by the currently configured protocols and features.

Never Alloc
Memory that has never been allocated.

Perm Alloc
Memory requested permanently by router tasks.

Temp Alloc
Memory allocated temporarily to router tasks.

Prev Alloc
Memory allocated temporarily and returned.

Number of global buffers:

Total Total number of global buffers in the system.

Free Number of global buffers available.

Fair Fair number of buffers for each interface. (See “Low”.)

Low The number of free buffers at which the allocation strategy changes to conserve buffers. If the value of *Free* is less than *Low*, then buffers will not be placed on any queue that has more than the *Fair* number of buffers in it.

Global buff size:
Global buffer size.

Data Maximum data link packet size of any interface.

Header
Sum of the maximum hardware, MAC, and data link headers.

Wrap Allowance given for MAC, LLC, or Network layer headers due to protocol wrapping.

Trailer Sum of the largest MAC and hardware trailers.

Total Overall size of each packet buffer

Network

Use the **network** command to enter the console environment for supported networks. This command obtains the console prompt for the specified interface. From the prompt, you can display statistical information, such as the LAN Emulation Clients for ATM networks.

Syntax:

network *interface#*

At the GWCON prompt (+), enter the **configuration** command to see the protocols and networks for which the router is configured. See “Configuration” on page 132 for more information on the configuration command.

Enter **interface** at the + prompt for a display of the networks for which the router is configured.

Enter the GWCON **network** command and the number of the interface you want to monitor or change. For example:

```
+network 0
ATM+
```

In the example, the ATM+ prompt is displayed. You can then view information about the ATM interface by entering the ATM operating commands.

After identifying the interface number of the interface you want to monitor, for interface-specific information, see the corresponding monitoring chapter in this manual for the specified network or link-layer interface. Console support is offered for the following network and link-layer interfaces:

- ATM
- Token-Ring LECs
- Ethernet LECs

Performance

Use the **performance** command at the GWCON prompt to enter the monitoring environment for performance. See “Chapter 15. Configuring and Monitoring Performance” on page 213 for more information.

Protocol

Use the **protocol** command to communicate with the router software that implements the network protocols installed in your router. The **protocol** command accesses a protocol’s command environment. After you enter this command, the prompt of the specified protocol appears. From the prompt, you can enter commands that are specific to that protocol.

Syntax:

protocol *prot#*

Enter the protocol number or short name as part of the command. To obtain the protocol number or short name, enter the CONFIG command environment (Config>), and then enter the **list configuration** command. See “Accessing the Configuration Process, CONFIG (Talk 6)” on page 14 for instructions on accessing Config>. To return to GWCON, enter **exit**.

See the corresponding monitoring chapter in this manual or in the *Multiprotocol Switched Services (MSS) Configuring Protocols and Features* for information on a specific protocol’s console commands.

Queue

Use the **queue** command to display statistics about the length of input and output queues on the specified interfaces. Information about input and output queues provided by the queue command includes:

- The total number of buffers allocated
- The low-level buffer value
- The number of buffers currently active on the interface.

Syntax:

queue *interface#*

To display information about one interface only, enter the interface or network number as part of the command. To obtain the interface number, use the GWCON **configuration** command.

Example:

queue

```
                Input Queue       Output Queue
Nt Interface  Alloc Low Curr    Fair Curr
0  Eth/0         30  10   30      30    1
1  PPP/0         24   4   24       4    0
2  FR/0          24   4   24       5    0
```

queue

```
               Input Queue       Output Queue
Nt Interface  Alloc Low Curr    Fair Curr
0  ATM/0         30  10   30      30    1
```

Nt Network interface number associated with the software.

Interface
Type of interface.

Input Queue:

Alloc Number of buffers allocated to this device.

Low Low water mark for flow control on this device.

Curr Current number of buffers on this device. The value will be 0 if the device is disabled.

Output Queue:

Fair Fair level for the length of the output queue on this device.

Curr Number of packets currently waiting to be transmitted on this device. For locally originated packets, the eligibility discard depends on the global low water mark described in the **memory** command.

The router attempts to keep at least the Low value packets available for receiving over an interface. If a packet is received and the value of Curr is less than Low, then the packet will be subject to flow control. If a buffer subject to flow control is to be queued on this device and the Curr level is greater than Fair, then the buffer is dropped instead of queued. The dropped buffer is displayed in the Output Discards column of the **error** command. It will also generate ELS event GW.036 or GW.057.

Due to the scheduling algorithms of the router, the dynamic numbers of Curr (particularly the Input Queue Curr) may not be fully representative of typical values during packet forwarding. The console code runs only when the input queues have

been drained. Thus, Input Queue Curr will generally be nonzero only when those packets are waiting on slow transmit queues.

Reset

Use the **reset** command to disable the specified interface and then re-enable it using new interface, protocol and feature configuration parameters. See “Resetting Interfaces” on page 90 for more information.

Syntax:

reset *interface#*

Statistics

Use the **statistics** command to display statistical information about the network software, such as the configuration of the networks in the router.

Syntax:

statistics *interface#*

To display information about one interface only, enter the interface or network number as part of the command. To obtain the interface number, use the GWCON **configuration** command.

Example:

```
statistics
                Unicast  Multicast      Bytes    Packets      Bytes
 Nt Interface  Pkts Rcv   Pkts Rcv   Received      Trans      Trans
 0  ATM/0           479          0      19730        479      20292
```

Nt Network interface number associated with the software.

Interface
Type of interface.

Unicast Pkts Rcv
Number of non-multicast, non-broadcast specifically-addressed packets at the MAC layer.

Multicast Pkts Rcv
Number of multicast or broadcast packets received.

Bytes Received
Number of bytes received at this interface at the MAC layer.

Packets Trans
Number of packets of unicast, multicast, or broadcast type transmitted.

Bytes Trans
Number of bytes transmitted at the MAC layer.

Test

Use the **test** command to verify the state of an interface or to enable an interface that was previously disabled with the **disable** command. If the interface is enabled and passing traffic, the **test** command will remove the interface from the network and run self-diagnostic tests on the interface.

Syntax:

test *interface#*

Note: For this command to work, you must enter the ***complete*** name of the command followed by the interface number.

Enter the interface or network number as part of the command. To obtain the interface number, use the GWCON **configuration** command. For example, when testing starts, the console displays the following message:

```
Testing net 0 ATM/0...
```

When testing completes or fails, or when GWCON times out (after 30 seconds), the following possible messages are displayed:

```
Testing net 0 ATM/0 ...successful
   Testing net 0 ATM/0 ...failed
  Testing net 0 ATM/0 ...still testing
   Network is already undergoing test, attempting restart
```

Some interfaces may take more than 30 seconds before testing is done.

Uptime

Use the **uptime** command to display time statistics about the router, including the following:

- Number of restarts.
- Number of known crashes.
- Whether the router was last reloaded or restarted.
- Time elapsed since the last reload.
- Time elapsed since the last restart.

Syntax:

uptime

Chapter 12. The Messaging (MONITR - Talk 2) Process

This chapter explains how to collect and display messages. (Refer to “Chapter 13. Using the Event Logging System (ELS)” on page 145 for information about ELS and message formats. Refer also to the *IBM 8210 Multiprotocol Switched Services Server Event Logging System Messages Guide* for a description of each message. This chapter includes the following sections:

- “What is Messaging (MONITR)?”
- “Commands Affecting Messaging”
- “Entering and Exiting the Messaging (MONITR) Process”
- “Receiving Messages”

What is Messaging (MONITR)?

The MONITR process provides a view of activity inside the router and the networks. MONITR also displays logging messages from the software.

Commands Affecting Messaging

The following commands affect the messaging process:

- OPCON commands:
  - **divert** temporarily diverts output to a different device.
  - **flush** causes the software to discard the messages it collects.
  - **halt** reverses the action of the divert command.
  - **talk** displays message output.
- CONFIG **set logging disposition** command sets the initial device to which the software sends its output.

Entering and Exiting the Messaging (MONITR) Process

To enter the messaging process from OPCON enter the **event** command or the **talk 2** command.

The console displays the messages the software has accumulated.

To exit messaging and return to OPCON, enter the OPCON intercept character (the default is **Ctrl-P**).

Receiving Messages

To receive messages at your console, enter the messaging process as described in the previous section. The software then displays all the messages it has recorded since it was last invoked. While you are connected to the messaging process, it displays all messages as they arrive.

Use the OPCON **divert** and **halt** commands to view software messages while you are doing something else with the router. Permitted devices divert output to TTY0 (the local console), TTY1, or TTY2 (the remote consoles).

© Copyright IBM Corp. 1996, 1998

Chapter 13. Using the Event Logging System (ELS)

This chapter describes the Event Logging System (ELS). The ELS continually logs all events, filtering them according to parameters that you select. A combination of operational counters and the ELS provides information for monitoring the health and activity of the system. The information is divided into the following sections:

- "What is ELS?"
- "Entering and Exiting the ELS Configuration Environment" on page 146
- "Event Logging Concepts" on page 146
- "Using ELS" on page 149
- "Using ELS to Troubleshoot a Problem" on page 151
- "Using and Configuring ELS Remote Logging" on page 153
- "Using ELS Message Buffering" on page 161

What is ELS?

ELS is a monitoring system and an integral part of the router operating system. ELS manages the messages logged as a result of router activity. Use ELS commands to set up a configuration that sorts out only those messages you feel are important. You can then display the messages on the console terminal screen, log them to a remote workstation, or send the messages to a network management station using Simple Network Management Protocol (SNMP) traps.

The ELS system and the operational counters are the best troubleshooting tools you have to isolate problems in the router. A quick scan of the event messages will tell you whether the router has a problem and where to start looking for it.

In the ELS configuration environment, the commands are used to establish a default configuration. This default configuration does not take effect until the router reinitializes.

Occasionally, it is helpful to temporarily view messages using parameters other than was set up in the ELS configuration environment, without having to reinitialize the router. The ELS operating and monitoring environment is used to:

- Temporarily change the default ELS display settings
  - Changes made in the ELS console environment take effect immediately
  - Changes made in the operating/monitoring environment are not stored in nonvolatile configuration storage.
- View statistical information regarding ELS uses of dynamic RAM

Note: Specific ELS messages are described in the *IBM 8210 Multiprotocol Switched Services Server Event Logging System Messages Guide*.

ELS is a subprocess that you access from the OPCON process.

© Copyright IBM Corp. 1996, 1998

Entering and Exiting the ELS Configuration Environment

The ELS configuration environment (available from the CONFIG process) is characterized by the `ELS Config>` prompt. Commands entered at this prompt create the ELS default state that takes effect after you restart the router. These commands are described in greater detail later in this chapter.

Configuration commands that have subsystem, group, or event as a parameter are executed in the following order:

- Subsystem
- Group
- Event

To set a basic ELS configuration, enter the **display subsystem all standard** command at the `ELS Config>` prompt. This command configures the ELS to display messages from all subsystems with the STANDARD logging level (that is, all errors and unusual informational comments).

Note: The router does not have a default ELS configuration. You must enter the ELS configuration environment and set the default state.

To enter the ELS configuration environment from OPCON:

1. Enter the **configuration** command. The console displays the CONFIG prompt (`Config>`). If the prompt does not appear when you first enter CONFIG, press **enter**.
2. At the CONFIG prompt, enter the following command to access ELS:

   ```
   Config> eve
   ```

   The console displays the ELS configuration prompt (`ELS config>`). Now, you can enter ELS configuration commands.

To leave the ELS configuration environment, enter the **exit** command.

Event Logging Concepts

This section describes how events are logged and how to interpret messages. Also described are the concepts of subsystem, event number, and logging level. A large part of ELS function is based on commands that accept the subsystem, event number, and logging level as parameters.

Causes of Events

Events occur continuously while the router is operating. They can be caused by any of the following reasons:

- System activity
- Status changes
- Service requests
- Data transmission and reception
- Data and internal errors

When an event occurs, ELS receives data from the system that identifies the source and nature of the event. Then ELS generates a message that uses the data received as part of the message.

Interpreting a Message

This section describes how to interpret a message generated by ELS. Figure 25 shows the message contents.

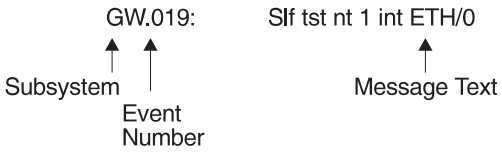


Figure 25. Message Generated by an Event

The information illustrated in Figure 25 as well as the ELS logging level information displayed with the **list subsystem** command is as follows:

Subsystem

Subsystem is a predefined short name for a router component, such as a protocol or interface. In Figure 25, **GW** identifies the subsystem through which this event occurred.

Other examples of subsystems include IP, TKR, and ATM. On a particular router, the actual subsystems present depend on the hardware and software configured for that router. You can use the **list subsystem** command described in this chapter to see a list of the subsystems on your router.

Enter the subsystem as a parameter to an ELS command when you want the command to affect the entire subsystem. For example, the ELS command **display subsystem GW** causes all events (except the events with 'debug' logging level) that occur through the GW subsystem to be displayed.

Event Number

Event Number is a predefined, unique, arbitrary number assigned to each message within a subsystem. In Figure 25, **019** is the event number within the GW subsystem. You can see a list of all the events within a subsystem by using the **list subsystem** command, where *subsystem* is the short name for the subsystem.

The event number always appears with a subsystem identifier, separated by a period. For example: **GW.019**. The subsystem and event number together identify an *individual* event. They are entered as a parameter to certain ELS commands. When you want a command to affect only the specified event, enter the subsystem and event number as a parameter for the ELS command.

Logging Level

Logging level is a predefined setting that classifies each message by the type of event that generated it. Use the **list subsystem** ELS console command to display the setting of the logging level. Table 12 on page 148 lists the logging levels and types. ERROR, INFO, TRACE, STANDARD, and ALL are aggregates of other logging level types.

STANDARD is the recommended default.

Table 12. Logging Levels

Logging Level	Type
UI ERROR	Unusual internal errors
CI ERROR	Common internal errors
UE ERROR	Unusual external errors
CE ERROR	Common external errors
ERROR	Includes all error levels above
UINFO	Unusual informational comment
CINFO	Common informational comment
INFO	Includes all comment levels above
STANDARD	Includes all error levels and all informational comment levels (default)
PTRACE	Per packet trace
UTRACE	Unusual operation Trace message
CTRACE	Common operation Trace message
TRACE	Includes all trace levels above
DEBUG	Message for debugging
ALL	Includes all logging levels

The logging level setting affects the operation of the following commands:

- **Display subsystem**
- **Nodisplay subsystem**
- **Trap subsystem**
- **Notrap subsystem**
- **Remote subsystem**
- **Noremote subsystem**

The logging level is set for a particular command when you specify it as a parameter to one of the above commands. For example:

```
display subsystem IP ERROR
```

Including the logging level on the command line modifies the **display** command so that whenever an event with a logging level of either UI-ERROR or CI-ERROR occurs through subsystem TKR, the console displays the resulting message.

You cannot specify the logging level for operations affecting groups or events.

Message Text

Message Text appears in short form. In Figure 25 on page 147, `Slf tst nt 1 int ETH/0` is the message generated by this event. Variables, such as *source_address* or *network*, are replaced with actual data when the message displays on the console.

The variable *error_code* is referred to by some of the Event Logging System message descriptions (usually preceded by rsn or reason). They indicate the type of packet error detected. Table 13 on page 149 describes the error or packet completion codes. Packet completion codes indicate the disposition of the packets received by the router.

Table 13. Packet Completion Codes (Error Codes)

Code	Meaning
0	Packet successfully queued for output
1	Random, unidentified error
2	Packet not queued for output due to flow control reasons
3	Packet not queued because network is down
4	Packet not queued to avoid looping or bad broadcast
5	Packet not queued because destination host is down (only on networks where this can be detected)

ELS displays network information as follows:

`nt 1 int Eth/0` (or) `network 1, interface Eth/0,`

where:

- 1 is the network number (each network on the router is numbered sequentially from zero).
- 0 is the unit number (the interfaces of each hardware type are numbered sequentially from zero).

Ethernet and 802.5 hardware addresses appear as a long hexadecimal number.

IP (Internet Protocol) addresses are printed as 4 decimal bytes separated by periods, such as 18.123.0.16.

Groups

Groups are user-defined collections of events that are given a name, the group name. Like the subsystem, subsystem and event number, and logging level, use the group name as a parameter to ELS commands. However, there are no predefined group names. You must create a group before you can specify its name on the command line.

To create a group, use the **add** configuration command, specify the name you want to call the group, and then specify the events you want to be part of the group. The events you add to the group can be from different subsystems and have different logging levels.

After creating a group, use the group name to manipulate the events in the group as a whole. For example, to turn off display of all messages from events that have been added to a group named grouptwo, include the group name on the command line, as follows:

```
nodisplay group grouptwo
```

To delete a group, use the **delete** command.

Using ELS

To use ELS effectively, do the following:

- Know what you want before using the ELS system. Clearly define the problem or events that you want to see before using the MONITR process.
- Execute the command **nodisplay subsystem all all** to turn off all ELS messages.

- Turn on only those messages that relate to the problem you are experiencing.
- Use the *IBM 8210 Multiprotocol Switched Services Server Event Logging System Messages Guide* to determine which messages are not normal.

When initially viewing ELS from the MONITR process, you will see a considerable amount of information. Because the router cannot buffer and display every packet under moderate to heavy loads the buffers are flushed. When this occurs the following message is displayed:

```
xx messages flushed
```

The router does not save these messages. When this message appears, tailor the ELS output to display only that information that is important to the current task you are monitoring, or use the advanced ELS commands to establish a message buffer. See "Using ELS Message Buffering" on page 161.

Managing ELS Message Rotation

It is also important to note that the ELS messages continually rotate through the router's buffers. To stop and restart the displaying of ELS messages, use the following key combinations:

Ctrl-S to pause scrolling

Ctrl-Q to resume scrolling

Ctrl-P to go back to the last process

You may also want to capture the ELS output to a file. You can do this by starting a script file or log file from your location when Telneting to a router. You can also do this by attaching a PC to the router's console port and starting a log file from within the terminal emulation package. This information is needed to help Customer Service diagnose a problem.

Capturing ELS Output Using a Telnet Connection on a UNIX Host

Use a Telnet connection on an AIX or UNIX host to capture the ELS messages on your screen to a file on the host. Before beginning, set up ELS for the messages you want to capture using the ELS console commands in "Chapter 14. Configuring and Monitoring the Event Logging System (ELS)" on page 165.

To capture the ELS output to a file on an AIX or UNIX host, follow these steps:

1. From the host, enter **telnet** *router_ip_addr* **| tee** *local_file_name*

   router_ip_addr is the IP address of the router

   local_file_name is the name of the file on the host where you want the ELS messages to be saved.

   The **tee** command displays the ELS messages on your screen and, at the same time, copies them to the local file.
2. From the OPCON prompt (*****), enter **t 2**. This accesses the MONITR process, which is the process that displays ELS messages on your screen. Depending on which ELS messages you configured, you should see ELS messages appearing on the screen.

   As long as you are in the MONITR process, all ELS messages will be written to the local file. When you exit the MONITR process (by entering **Ctrl-P**) or terminate the Telnet session, the logging of messages to the local file will stop.

You can also use remote logging instead of capturing ELS output on a UNIX Host. For more information about remote logging, see “Using and Configuring ELS Remote Logging” on page 153.

Configuring ELS So Event Messages Are Sent In SNMP Traps

ELS can be configured so that event messages are sent to a network management workstation in an SNMP enterprise-specific trap. These traps are useful for reporting status and diagnostic results, and are often used for remote monitoring of a IBM 8210. When ELS is configured appropriately, an SNMP trap will be generated each time the selected event occurs. For more information about SNMP, see *Multiprotocol Switched Services (MSS) Configuring Protocols and Features*.

To tell ELS that a specific event should be activated to be sent as an SNMP trap, at the `ELS config>` prompt or at the `ELS>` prompt, using IP as an example, type:

```
trap event ip.007
```

Note: If you are at the `ELS config>` prompt, you will need to reboot.

To enable the ELS enterprise-specific trap, follow these steps:

1. At the `SNMP config>` prompt, using **public** as an example, type:

   ```
   SNMP config> add address public <network manager IP address>
   SNMP config> enable trap enterprise public
   SNMP config> set community access read_trap public
   ```

   Note: You need to reboot to activate these changes.
2. Enable your network management station to receive and properly display the enterprise-specific traps.

Follow these steps to trap groups, subsystems, and events.

Using ELS to Troubleshoot a Problem

If you are trying to troubleshoot a particular problem, display the messages related to the problem. For example, if experiencing a problem with bridging, turn on the bridging messages:

display subsystem srt all

display subsystem br all

Initially, because of the rapid pace of messages scrolling across the screen, you may want to record the numbers you see and look them up in the *Event Logging System Messages Guide* manual. Once you become familiar with different types of messages being displayed for a particular protocol, you can turn on and turn off only those messages that contain the information that you require to troubleshoot a problem. The following sections list specific ELS examples. Keep in mind that different problems may require different steps.

ELS Example 1

You are interested in looking at the frequency of polling on a Token-Ring interface, and finding out whether the polls are successful.

Using ELS

```
ELS> nodisplay subsystem all all
ELS> display subsystem tkr all
Ctrl-P
* t 2
```

As the messages begin to scroll by, look for ELS message tkr.031.

ELS Example 2

SRB bridging is not working.

1. Check the configuration.
2. Use the GWCON bridging console to verify that the bridging interfaces are enabled.
3. Enter:

   ```
   * t 6
   config> event
   ELS config> nodisplay subsystem all all
   ELS config> display subsystem srb all
   ELS config> exit
   config> Ctrl-P
   ```

4. Restart the routing subsystem. When the subsystem has restarted, enter the following:

   ```
   * t 2
   ```

ELS Example 3

Router cannot communicate with an IPX server on an Ethernet.

1. Enter the **talk** command and the PID for GWCON.

   ```
   * talk 5
   ```

   The console displays the GWCON prompt (+). If the prompt does not appear when you first enter GWCON, press **Return**.
2. At the GWCON prompt (+), enter **IPX** to access the IPX console prompt (IPX>).
3. At the IPX console prompt, enter the **slist** command to verify that the server is listed. (See the section on monitoring IPX in the *Multiprotocol Switched Services (MSS) Configuring Protocols and Features* for information on the **slist** command.)
4. Check the IPX configuration.
5. Enter the following:

   ```
   * t 5
   + event
   ELS> nodisplay subsystem all all
   ELS> display subsystem IPX all
   ELS> display subsystem eth all
   ELS> Ctrl-P
   * t 2
   ```

As the messages begin to scroll by, look for ELS message eth.001. This indicates that the server has a bad Ethernet type field.

Using and Configuring ELS Remote Logging

The remotely-logged ELS message contains all of the information that is contained in ELS messages found in the monitor queue, as viewed under `talk 2`, and also contains additional information as shown in Figure 26.

```
Date/Time         IP address      Sequence Number      Local Name      ELS Subsystem Name, &
                  assigned        used for detecting   assigned        Formatted message
                  by the user     missing messages     by the user

Nov 20 12:13:47   5.1.1.1         Msg [0444] from      ** IBM/8210 **  :els: MPC.011 Del ent ...
```

Figure 26. Syslog Message Description

Note the following differences in the remote log display:

- The month and day of month in addition to the time, which is always displayed as the time-of-day.
- An IP address, which is the user-specified source IP address. If a DNS server resolves the source IP address to a hostname, then the hostname will be displayed instead of the IP address.
- A Sequence number is added to the message by the source device to assist in detecting dropped messages. See “Remote Logging Output” on page 157 for an explanation of dropped messages. When the sequence number of the message reaches 9999, the next sequence number is 0001.
- A “Local Name” for the source router, to assist in distinguishing between messages from multiple sources. If you do not configure a local name, this field is blank.

Syslog Facility and Level

Remotely-logged ELS messages are transmitted over the network in UDP packets with the destination port number in the UDP header always equal to 514, the syslog port. To receive and process the UDP packets, the *syslog daemon* (syslogd) must be running in the remote workstation that is receiving and logging the ELS messages. See “Remote Workstation Configuration” for details.

Although it is not displayed in the remotely-logged ELS message, every ELS message sent on the network in a UDP packet must be assigned a *syslog_facility* and a *syslog_level*. The syslog daemon uses the combination of facility and level to determine where to route the message. Typically, you want the ELS messages to be written to one or more files in the remote host. Other options include displaying the message on the console, sending the message to one or more users, or sending the message to another workstation.

The commands you use to specify the *syslog_facility* and *syslog_level* values, along with other remote-logging related console commands, are described in “ELS Monitoring Commands” on page 184 and “ELS Configuration Commands” on page 165. Review these commands before reading through the next section.

Remote Workstation Configuration

The following configuration assumes that a single 8210 is remote-logging to a single remote workstation. You can configure multiple 8210s to remote-log to the same

remote workstation. However, a particular 8210 can log to one and only one remote workstation. The operating system used in this example is AIX 4.2. Your environment may be slightly different. For more information on syslog, refer to the documentation for your operating system.

To perform the configuration on an AIX workstation, you must log in as **root**. To configure the workstation:

1. Create or edit a syslog.conf file to specify where ELS messages with particular *syslog_facility* and *syslog_level* values are to be written. See the bottom of Figure 27 on page 155 for an example of how to specify the message destination. Note that the full pathname of the log files must be specified. The default location for the syslog configuration file is /etc/syslog.conf.
2. Create the files for logging syslog messages that you specified in the syslog.conf file.
3. Start the syslog daemon by entering **syslogd**. To start the syslog daemon from SRC (System Resource Controller), enter **startsrc -s syslogd**. If the pathname of the configuration file is not /etc/syslog.conf, then enter **syslogd -f** *pathname*. To start the syslog daemon in debug mode, enter **syslogd -d**.

   Note: Running multiple instances of the syslog daemon is not supported.
4. If the syslog daemon is already running when you create or modify the syslog.conf file, it must be restarted so that the daemon reinitializes the configuration from syslog.conf.
5. Verify the setup by using the **logger** command as follows:

   ```
   logger -p user.alert  THIS IS A TEST MESSAGE (user.alert)
   logger -p news.info  THIS IS A TEST MESSAGE (news.info)
   ```

   If the setup is correct, `THIS IS A TEST MESSAGE...` will be written to the files specified in syslog.conf.

```
# @(#)34       1.9 src/bos/etc/syslog/syslog.conf, cmdnet, bos411, 9428A410j 6/13/93 14:52:39
#
# COMPONENT_NAME: (CMDNET) Network commands.
#
# FUNCTIONS:
#
# ORIGINS: 27
#
# (C) COPYRIGHT International Business Machines Corp. 1988, 1989
# All Rights Reserved
# Licensed Materials - Property of IBM
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#
# /etc/syslog.conf - control output of syslogd
#
# Each line must consist of two parts:-
#
# 1) A selector to determine the message priorities to which the
#    line applies
# 2) An action.
#
# The two fields must be separated by one or more tabs or spaces.
#
# format:
#
# <msg_src_list>               <destination>
#
# where <msg_src_list> is a semicolon separated list of <facility>.<priority>
# where:
#
# <facility> is:
#      * - all (except mark)
#      kern,user,mail,daemon, auth, syslog, lpr, news, uucp, cron, authpriv, local0 - local7
#
# <priority or level> is one of (from high to low):
#      emerg,alert,crit,err(or),warn(ing),notice,info,debug
#      (meaning all messages of this priority or higher)
#
# <destination> is:
#      /filename - log to this file
#      username[,username2...] - write to user(s)
#      @hostname - send to syslogd on this machine
#      * - send to all logged in users
#
# example:
# "mail messages, at debug or higher, go to Log file. File must exist."
# "all facilities, at debug and higher, go to console"
# "all facilities, at crit or higher, go to all users"
#  mail.debug          /usr/spool/mqueue/syslog
#  *.debug             /dev/console
#  *.crit                      *

#   syslog messages with facilty / priority values of LOG_USER,   LOG_ALERT
user.alert            /tmp/syslog_user_alert

#   syslog messages with facilty / priority values of LOG_NEWS,  LOG_INFO
news.info           /tmp/syslog_news_info
```

Figure 27. syslog.conf Configuration File

Configuring the 8210 for Remote Logging

To configure a 8210:

1. In talk 6, configure the remote-logging facility as shown in Figure 28 on page 156. The IP address specified as the *source-ip-addr* should be an IP address that is configured in the 8210 for easier identification when the IP address or the hostname is shown in the remotely-logged ELS message. You should also verify that this IP address resolves quickly into a hostname by the

name server or that the name server at least responds quickly with “address not found.” To determine whether this happens, issue the **host** command on your workstation as follows:

```
workstation> host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

If the response takes more than 1 second, select an IP address which resolves more quickly.

2. In talk 6 configure events and subsystems for remote-logging, as shown in Figure 29 on page 157.
3. Write the configuration and reload the 8210.

```
ELS config>set remote source-ip-addr 5.1.1.1
Source IP Addr = 5.1.1.1

ELS config>set remote remote-ip-addr 192.9.200.1
Remote Log IP Addr = 192.9.200.1

ELS config>set remote local-id ** IBM/8210 **
Remote Log Local ID = ** IBM/8210 **

ELS config>set remote no-msgs-in-buffer 100
Number of messages in Remote Log Buffer must be 100-512
Number of Messages in Remote Buffer = 100

ELS config><B>set remote facility log_news
Default Syslog Facility = LOG_NEWS

ELS config>set remote level log_info
Default Syslog Level = LOG_INFO

ELS config>set remote on
Remote Logging is ON

ELS config>list remote

------------------   Remote Log Status  -----------------

Remote Logging is ON
Source IP Address = 5.1.1.1
Remote Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_NEWS
Default Syslog Priority Level = LOG_INFO
Number of Messages in Remote Log =  100
Remote Logging Local ID = ** IBM / 8210 **
ELS config>
```

Figure 28. Configuring the 8210 for Remote Logging

```
ELS config>display sub snmp all
ELS config>remote sub snmp all log_news log_info

ELS config>display event srt.017
ELS config>remote event srt.017 log_news log_info

ELS config>display event stp.016
ELS config>remote event stp.016 log_user log_info

ELS config>display event stp.026
ELS config>remote event stp.026 log_news log_info

ELS config>display event stp.024
ELS config>remote event stp.024 log_news log_info

ELS config>display event ip.068
ELS config>remote event ip.068 log_news log_info

ELS config>display event ip.058
ELS config>remote event ip.058 log_news log_info

ELS config>display event ip.022
ELS config>remote event ip.022 log_news log_info

ELS config>display event gw.022
ELS config>remote event gw.22 log_news log_info

ELS config>display event arp.011
ELS config>remote event arp.011 log_user log_alert

ELS config>display event arp.002
ELS config>remote event arp.022 log_user log_alert

ELS config>list status
Subsystem:    SNMP
Disp levels:  ERROR INFO TRACE
Trap levels:  none
Trace levels: none
Remote levels:  ERROR INFO TRACE
        Syslog Facility/Level: LOG_NEWS LOG_INFO

Event     Display Trap    Trace     Remote
SRT.017   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.016   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.026   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.024   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.068    On      Unset   Unset
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.058    On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.022    On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
GW.022    On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
ARP.011   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_USER LOG_ALERT
ARP.002   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_USER LOG_ALERT
```

Figure 29. Configuring Subsystems and Events for Remote Logging

Remote Logging Output

Figure 30 on page 158 shows a sample from the /tmp/syslog_news_info file. Notice that the first message has a sequence number of 310. This means that the first 309 ELS messages were not sent from the source 8210. There are several reasons for this:

- The remote-logging facility had not completed initialization when the messages were first passed to ELS

- A route from the source 8210 to the remote workstation was not in the routing table
- The interface for the outbound UDP packet containing the ELS messages was not in the "Up" state

Notice in **1** that messages 311-313 did not get remote-logged. This is because an ARP request was outstanding and until the ARP response is received, all but the first packet is dropped in the source 8210. Additionally, the ARP cache is cleared at a user-configured refresh rate, and a new ARP request is issued. To determine when this is occurring, you can remote log events ARP.002 and ARP.011 in addition to the primary ELS events of interest. Figure 32 on page 159 shows ARP events logged to the *syslog_user_alert* file that account for events 445 and 446, which were indicated as missing in Figure 30.

```
Nov 20 12:03:16 workstа01 root:  THIS IS A TEST MESSAGE  (news.info)
Nov 20 12:08:48 5.1.1.1 Msg [0310] from ** IBM / 8210 **: els:  IP.022: add nt 192.9.200.0 int 192.9.200.20
nt 0 int Eth/0

 1  ( messages 311, 312, and 313 did not get remote-logged due to ARP request outstanding - see
  explanation in the text)

 2  (messages 314 and 315 were logged to a separate
file - see explanation in the text)

Nov 20 12:08:48 5.1.1.1 Msg [0316] from ** IBM / 8210 **: els:  IP.068: routing cache cleared
Nov 20 12:08:48 5.1.1.1 Msg [0317] from ** IBM / 8210 **: els:  IP.022: add nt 5.0.0.0 int 5.1.1.1 nt 5 int Eth/4
Nov 20 12:08:48 5.1.1.1 Msg [0318] from ** IBM / 8210 **: els: SRT.017: Enabling SRT on port 5 nt 5 int Eth/4


(message 319 was logged to a separate file)

Nov 20 12:08:48 5.1.1.1 Msg [0320] from ** IBM / 8210 **: els:  IP.068: routing cache cleared

(120 messages not shown)

Nov 20 12:13:33 5.1.1.1 Msg [0441] from ** IBM / 8210 **: els:  GW.022: Nt fld slf tst nt 3 int Eth/3
Nov 20 12:13:33 5.1.1.1 Msg [0442] from ** IBM / 8210 **: els:  GW.022: Nt fld slf tst nt 6 int Eth/5
Nov 20 12:13:38 5.1.1.1 Msg [0443] from ** IBM / 8210 **: els:  GW.022: Nt fld slf tst nt 11 int ISDN/0


(messages 444 and 447 were logged to a separate file)


(messages 445 and 446 did not get remote-logged due to ARP request outstanding)

Nov 20 12:13:50 5.1.1.1 Msg [0448] from ** IBM / 8210 **: els:  GW.022: Nt fld slf tst nt 4 int PPP/0
Nov 20 12:13:50 5.1.1.1 Msg [0449] from ** IBM / 8210 **: els:  IP.068: routing cache cleared
Nov 20 12:13:50 5.1.1.1 Msg [0450] from ** IBM / 8210 **: els:  IP.058: del nt 4.0.0.0 rt via 0.0.0.4 nt 4 int PPP/0
```

Figure 30. Sample Contents from Syslog News Info File

If the initial ELS messages that are generated during and immediately after booting are of particular interest, then it is recommended that these messages also be displayed in the monitor queue, which is viewed with talk 2. Figure 31 on page 159 shows the talk 2 output including the initial messages that did not get remote-logged. Note that there is a message in the talk 2 output that indicates that the remote-logging facility is available. This does not indicate that a route exists to the remote workstation, nor that the associated interface is in the "Up" state. It simply provides a reference point before which no messages can be successfully remote-logged.

Also notice that you can account for the messages that were missing (indicated in Figure 30 with **2**) in the talk 2 output.

```
12:08:17 SNMP.024: generic trc (P2) at snmp_mg.c(766): Now 0 trap destinations
12:08:17 SNMP.012: comm public added
12:08:17 SNMP.012: comm public added
12:08:27 SNMP.022: ext err (Z1) at snmp_resconf.c(322): add_router_if_info(): sr
rdrec failed

12:08:27 SNMP.022: ext err (Z1) at snmp_resconf.c(322): add_router_if_info(): sr
rdrec failed

12:08:27 SNMP.028: err (E2) at snmp_moh.c(1583) : Duplicate
12:08:27 SNMP.028: err (E2) at snmp_moh.c(1583) : Duplicate
12:08:28   GW.022: Nt fld slf tst nt 13 int PPP/3
12:08:28   IP.022: add nt 4.0.0.0 int 4.1.1.1 nt 4 int PPP/0

     ( 297 messages not shown )                                    Corresponding Sequence
                                                                   Numbers in
12:08:43   GW.022: Nt fld slf tst nt 12 int PPP/2                  Remote-Logging Files :
12:08:43   GW.022: Nt fld slf tst nt 13 int PPP/3
12:08:48   IP.022: add nt 192.9.200.0 int 192.9.200.20 nt 0 int Eth/0   [0310] first message logged
12:08:48  SRT.017: Enabling SRT on port 1 nt 0 int Eth/0          -- not logged (ARP request) --
12:08:48  STP.016: Select as root TB-1, det topol chg            -- not logged (ARP request)--
12:08:48  STP.026: Root TB-1, strt hello tmr                     -- not logged (ARP request)--
12:08:48  ARP.002: Pkt in 1 1 800 nt 0 int Eth/0                 [0314]
12:08:48  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0                 [0315]
12:08:48   IP.068: routing cache cleared                         [0316]


     ( 126 messages not shown )

12:13:38   GW.022: Nt fld slf tst nt 11 int ISDN/0               [0443]
12:13:47  ARP.011: Del ent 1 3 nt 0 int Eth/0                    [0444]
12:13:47  ARP.011: Del ent 1 3 nt 0 int Eth/0                    -- not logged (ARP request) --
12:13:47  ARP.002: Pkt in 1 1 800 nt 5 int Eth/4                 -- not logged (ARP request)--
12:13:47  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0                 [0447]
12:13:50   GW.022: Nt fld slf tst nt 4 int PPP/0                 [0448]
```

Figure 31. Output from Talk 2

You can use the timestamp, which appears in both the remote-logging output file and the talk 2 output, to determine when the first ELS message is successfully remote-logged. To use the timestamp for this purpose, configure ELS such that the timestamp in the monitor queue displays the time-of-day.

Also notice in Figure 30 on page 158 that messages 311-313 did not get remote-logged. This is because an ARP request was outstanding and until the ARP response is received, all but the first packet is dropped in the source IBM 8210. The ARP cache is cleared at a user-configured refresh rate, and the device issues a new ARP request. To determine when ARP requests are occurring, events ARP.002 and ARP.011 can be remote-logged, in addition to the ELS events of interest. Figure 32 shows ARP events logged to the *syslog_user_alert* file that account for events 445 and 446, which were indicated as missing in Figure 30 on page 158.

```
Nov 20 12:02:53 worksta01 root: THIS IS A TEST MESSAGE (user.alert)
Nov 20 12:08:48 5.1.1.1 Msg [0314] from ** IBM / 8210 **: els:  ARP.002: Pkt in 1 1 800 nt 0 int Eth/0
Nov 20 12:08:48 5.1.1.1 Msg [0315] from ** IBM / 8210 **: els:  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
Nov 20 12:08:48 5.1.1.1 Msg [0319] from ** IBM / 8210 **: els:  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
Nov 20 12:13:47 5.1.1.1 Msg [0444] from ** IBM / 8210 **: els:  ARP.011: Del ent 1 3 nt 0 int Eth/0
Nov 20 12:13:47 5.1.1.1 Msg [0447] from ** IBM / 8210 **: els:  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
```

Figure 32. Sample Contents from Syslog_user_alert File

You can prevent the loss of ELS messages caused by this ARP sequence by establishing a static relationship between the IP address and the MAC address. The basic steps are outlined below and are illustrated in Figure 33 on page 160.

1. In talk 5, “ping” the remote workstation’s IP address
2. In talk 5, determine the interface (net) number used to send messages to the remote-workstation’s IP address
3. Use the net number from the previous step to determine the associated MAC address

4. In talk 6, add an ARP entry to establish a static IP address to MAC address relationship

```
*t 5
+p ip

IP>ping 192.9.200.1
PING 192.9.200.20 -> 192.9.200.1: 56 data bytes, ttl=64, every 1 sec.
56 data bytes from 192.9.200.1: icmp_seq=0. ttl=64. time=0. ms
----192.9.200.1 PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms

IP>dump

  Type   Dest net            Mask          Cost    Age       Next hop(s)
.
   Dir*  192.9.200.0         FFFFFF00      1       102305    Eth/0
.
IP>exit
+int
                                                    Self-Test  Self-Test   Maintenance
Net   Net'   Interface  Slot-Port                   Passed     Failed      Failed
0     0      Eth/0      Slot: 1   Port: 1               1          0           0
.
+p arp
ARP>dump
Network number to dump [0]? 0
Hardware Address        IP Address        Refresh
02-60-8C-2D-69-5D       192.9.200.1       2

Ctrl-P
*t 6
config>p arp
ARP config>add entry
Interface Number [0]? 0
Protocol [IP]? IP
IP Address [0.0.0.0]? 192.9.200.1
Mac Address []? 02608C2D695D
ARP config> list entry

Mac address translation configuration

IF #      Prot #  Protocol -> Mac address
   0           0  192.9.200.1 -> 02608C2D695D
ARP config>exit
Config>write

Ctrl-P

*reload
Are you sure you want to reload the gateway? (Yes or [No]): Yes

 (after reload, static ARP entry is active)
```

Figure 33. Example of Setting Up a Static ARP Entry

Additional Considerations

ELS Messages Containing IP Addresses

ELS messages containing an IP address which matches the IP address of the remote workstation will not be remote-logged, even if configured for remote-logging, and may appear under talk 2. These messages are discarded instead of being remote-logged in order to prevent excessive UDP packets from being sent on the network.

Duplicate Logging

If a facility value is repeated in *syslog.conf*, for example:

```
user.debug        /tmp/syslog_user_debug
user.alert        /tmp/syslog_user_alert
```

The syslog daemon will log *user.debug* messages only to the */tmp/syslog_user_debug* file while user.alert messages will be logged to both the */tmp/syslog_user_debug* file and the */tmp/syslog_user_alert* file. This is consistent with the syslog design that logs the more severe conditions in multiple places.

To prevent this duplicate logging, it is recommended that different facility values be specified in the *syslog.conf* file. A total of 19 facility values are available.

Recurring Sequence Numbers in Syslog Output Files

Depending upon the configuration of your network, it is possible for duplicate UDP packets containing ELS messages to arrive at the remote host. It is also possible for the packets to arrive in a different order than they were transmitted. An example of this phenomenon is shown in Figure 34. Notice that the messages with sequence numbers 628 through 633 are logged twice. Also notice that after the first occurrence of sequence number 0630, sequence number 0629 occurs again, followed by the second occurrence of 0630.

```
Apr 01 10:48:33 0.0.0.0 Msg [0628] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:48:33 0.0.0.0 Msg [0628] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0629] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0630] from: RA22: : els: IPX.018: SAP gen rply sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0629] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0630] from: RA22: : els: IPX.018: SAP gen rply sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0631] from: RA22: : els: IPX.037: RIP resp sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0631] from: RA22: : els: IPX.037: RIP resp sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0632] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0632] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:50:08 0.0.0.0 Msg [0633] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:50:08 0.0.0.0 Msg [0633] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
```

Figure 34. Example of Recurring Sequence Numbers in Syslog Output

Because neither Syslog nor UDP has the ability to handle duplicate or out of sequence packets, it is important to recognize the possibility of duplicate sequence numbers occurring.

Using ELS Message Buffering

Message buffering is an advanced feature of ELS that can help you with problem determination. You can set up defaults that ELS will use for message buffering or change how messages are buffered while the router is operating. Message buffering can minimize the information lost because messages have wrapped in the default message buffers. Message buffering is accessible through the **advanced** configuration or monitoring command. It enables you to:

- Specify whether buffering is active.
- Specify what events are written to the message buffer.
- Stop buffering and free the memory allocated for buffering.
- Display the status of the message buffer.
- Specify an event that stops message buffering and what action the system takes when the event occurs.

- Send a formatted version of the buffer to a file at a remote server.
- View a specific number or all of the ELS messages in the buffer.
- Write the buffer to a hard drive if a hard drive is present.
- Read a file that contains a formatted ELS message buffer from the hard drive , if a hard drive is present.
- Send a file that contains a formatted ELS message buffer from the hard drive , if a hard drive is present.

For specifics about the commands, see “ELS Message Buffering Configuration Commands” on page 180 and “ELS Message Buffering Monitoring Commands” on page 207.

The following example shows how to configure ELS message buffering.

```
 MOS Operator Console

For help using the Command Line Interface, press ESCAPE, then '?'

 *t 5 :Enter t 5 at the * prompt.

 CGW Operator Console

 +ev :Enter ev at the + prompt.
 Event Logging System user console
 ELS>a :Enter a for advanced at the ELS prompt.
 Advanced ELS Console
 ELS Advanced>li s :Enter li s to list status at the > prompt.
 ------------------Advanced ELS Configuration-----------------------
 Logging Status:  OFF  Wrap Mode:  ON   Logging Buffer Size: 0 KB
 Stop-Event:  NONE   Stop-String:   NONE
 Additional Stop-Action:  NONE
 -----------------------Run-Time Status-----------------------------
 Has Stop Condition Occurred?   NO   Messages currently in buffer:  0

 ELS Advanced>s b :Enter s b to set buffer size.
 Enter buffer size of 0 KB or between 148 and 593 KB [148]?
 Buffer size set to 148 KB
 ELS Advanced>s s e gw.26 :Enter s s e to set stop event eg. gw.26
 Stop Event "GW.026" has been set
 ELS Advanced>ex :Enter ex to exit Advanced to list gw.26
 ELS>list ev gw.26
 Level: C-TRACE
 Message: Mnt nt %n int %s/%d
 Active:         Count: 742

 ELS>a :Enter a to get back to advanced.
 Advanced ELS Console
 ELS Advanced>s s s Mnt nt 5 :Enter s s s to set the stop string.
 Stop String set to "Mnt nt 5"
 ELS Advanced>s s a ? :Enter s s a ? to query available stop actions.
 NONE
 APPN-DUMP  :Only available if APPN active and in the load image.
 SYSTEM-DUMP
 ELS Advanced>s s a s :Enter s s a s to set SYSTEM-DUMP stop action.
 Stop Action has been set to SYSTEM-DUMP
 ELS Advanced>s w off to :Enter s w on to set wrap mode off.
 Advanced Wrap Mode set to OFF.

 ELS Advanced>log sub gw all :Enter to enable the whole gw subsystem
 ELS Advanced>s l on :Enter s l on to start the logging process.
 Advanced Logging set to ON.
 ELS Advanced>li s :Enter to list status of logging.
 ------------------Advanced ELS Configuration-----------------------
 Logging Status:  OFF  Wrap Mode: OFF  Logging Buffer Size: 148 KB
 Stop-Event:     GW.026   Stop-String:  Mnt nt 5
 Additional Stop-Action:  SYSTEM-DUMP


-----------------------Run-Time Status-----------------------------
 Has Stop Condition Occurred?   YES  Messages currently in buffer:  7

 ELS Advanced>v a n :Enter to view all messages in buffer. For this
                     trivial example any viewing command suffices.
```

```
 1  10:52:10   GW.026: Mnt nt 0 int Eth/0
 2  10:52:10   GW.026: Mnt nt 5 int Eth/1->This triggers stop action
 3  10:52:14   GW.026: Mnt nt 0 int Eth/0  Note that 5 more events
 4  10:52:14   GW.026: Mnt nt 5 int Eth/1  get logged before
 5  10:52:18   GW.026: Mnt nt 0 int Eth/0  logging stops and
 6  10:52:18   GW.026: Mnt nt 5 int Eth/1  the stop action occurs.
 7  10:52:22   GW.026: Mnt nt 0 int Eth/0

Bughlt: Dump initiated by ELS Stop Action.

BUGHLT+80; Dump initiated by ELS Stop Action.

Note:
In reality if the stop action is the SYSTEM-DUMP you will not be
able to list the final status as above nor view the buffer because
the router will be attempting to reload.
```

Using ELS

Chapter 14. Configuring and Monitoring the Event Logging System (ELS)

This chapter describes how to configure events logged by ELS and how to use the ELS commands. The information includes the following sections:

- "Accessing the ELS Configuration Environment"
- "ELS Configuration Commands"
- "Entering and Exiting the ELS Operating Environment" on page 184
- "ELS Monitoring Commands" on page 184

For more information on the Event Logging System and how to interpret ELS event messages, refer to "Chapter 13. Using the Event Logging System (ELS)" on page 145.

Accessing the ELS Configuration Environment

The ELS configuration environment is characterized by the `ELS config>` prompt. Commands entered at this prompt are described "Chapter 14. Configuring and Monitoring the Event Logging System (ELS)".

To enter the ELS configuration environment:

1. Enter **configuration**.

   The monitoring displays the `Config>` prompt. If the prompt does not appear, press **enter**.
2. At the `Config>` prompt, enter the following command to access ELS:

   ```
   event
   ```

   The monitoring displays the ELS configuration prompt (`ELS config>`). Now, you can enter ELS configuration commands.

To leave the ELS configuration environment, enter the **exit** command.

ELS Configuration Commands

Table 14 summarizes the ELS configuration commands. The remainder of this section describes each one in detail. After accessing the ELS configuration environment, you can enter ELS Configuration commands at the `ELS Config>` prompt.

Table 14. ELS Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Add	Adds an event to an existing group or creates a new group.
Advanced	Places you in the advanced configuration environment in which you can configure message buffering.
Clear	Clears all ELS configuration information.
Default	Resets the display or trap setting of an event, group, or subsystem.

© Copyright IBM Corp. 1996, 1998

Table 14. ELS Configuration Command Summary (continued)

Command	Function
Delete	Deletes an event number from an existing group or deletes an entire group.
Display	Enables message display on the console monitor.
List	Lists information on ELS settings and messages.
Nodisplay	Disables message display on the console.
Noremote	Disables remote logging to a remote workstation.
Notrace	Controls disablement of packet trace events.
Notrap	Keeps messages from being sent out in SNMP traps.
Remote	Allows messages to be logged to a remote workstation.
Set	Sets the pin parameter and the timestamp feature options.
Trace	Controls enablement of packet trace events.
Trap	Allows messages to be sent to a network management workstation in SNMP traps.
View	Allows viewing of traced packets.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to add an individual event to an existing group or to create a new group. Group names must start with a letter and are case sensitive. You cannot append an entire subsystem to a group.

Syntax:

add *group_name subsystem.event_number*

Note: If the specified group does not exist, the following prompt asks you to confirm the creation of a new group:

```
Group not found. Create new group? (yes or no)
```

Advanced

Use the **advanced** command to enter the advanced configuration environment. In this environment you configure message buffering.

Syntax:

advanced

Clear

Use the **clear** command to clear all of the ELS configuration information.

Syntax:

clear

Example:

```
clear

You are about to clear all ELS configuration information
Are you sure you want to do this (Yes or No):
```

Default

Resets the display or trap setting of an event, group, or subsystem back to a disabled state.

Syntax:

default display
trap
remote

display *event* **OR** *group* **OR** *subsystem*
Controls the output of the display of messages to the monitoring.

trap *event* **OR** *group* **OR** *subsystem*
Controls the generation of traps to the network management station.

remote *event* **OR** *group* **OR** *subsystem*
Controls the generation of traps to the remote station.

Delete

Use the **delete** command to delete an event number from an existing group or to delete the entire group. If the specified event is the last event to be deleted in a group, you will be notified. If *all* is specified instead of *subsystem.event_number*, a prompt asks you to confirm the deletion of the entire group.

Syntax:

delete *group_name subsystem.event_number*

Display

Use the **display** command to enable message displaying on the monitoring monitor for specific events, a range of events for a subsystem, groups, or subsystems.

Syntax:

display event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Displays messages of the specified event (*subsystem.event#*).

group *groupname*
Displays messages of a specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event in the specified event range.

Displays a range of messages for the specified subsystem.

Example:

```
display range gw 19 22
```

Displays events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystemname*
Displays messages associated with the specified subsystem. To find out which subsystems are on the router, type **list subsystems**.

Note: Although ELS supports all subsystems on the router, not all devices support all subsystems. See *Event Logging System Messages Guide* for a list of currently supported subsystems.

List

Use the **list** command to get updated information regarding ELS settings and listings of selected messages.

Syntax:

list all
groups
pin
remote-log status
status
subsystem . . .
subsystems all
trace-status

all Lists information from all the **list** categories.

groups
Lists the user-defined group names and contents.

pin Lists the current number of ELS event messages sent in SNMP traps (per second).

remote-log status
Lists the current values of remote logging options.

Example:

```
list r

Remote Logging is ON
Source IP Address = 192.67.38.2
Remote Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_DAEMON
Default Syslog Priority Level = LOG_CRIT
Number of Messages in Remote Log = 256
Remote Logging Local ID = MYHOSTNAME
```

status Lists the subsystems, groups, and events that have been modified by the **display**, **nodisplay**, **trap**, **notrap**, **trace**, **notrace**, **remote**, and **noremote** commands.

Example:

```
list status

Subsystem:            TKR
Disp Levels:          STANDARD
Trap levels:          none
Trace levels:         none
Remote levels:        ERROR INFO TRACE
```

```
Syslog Facility/Level: LOG_USER LOG_INFO

Group        Disp     Trap    Trace  Remote
Mygroup     Unset    Unset    Unset    On
                                       Syslog Facilty/Level: LOG_DAEMON LOG_CRIT

Event        Disp     Trap    Trace  Remote
IP.007      Unset    Unset    Unset    On
                                       Syslog Facility/Level: LOG_CRON LOG_NOTICE
```

Note: Not only is remote logging enabled, but the display includes the Syslog Facility/Level values for each subsystem, group, and event. Ranges of events are listed as individual events.

subsystem
Lists names, events, and descriptions of all subsystems.

(Example output from a **list subsystem** command can be found beginning on page 188.)

subsystem *subsystem*
Lists all events in a specified subsystem.

Example:

```
list subsystem gw


Event      Level      Message

GW.001     ALWAYS   Copyright 1984 Mass Institute of Technology
GW.002     ALWAYS   Portable CGW %s Rel %s strtd
GW.003     ALWAYS   Unus pkt len %d nt %d int %s/%d
GW.004     ALWAYS   Sys %s q adv alloc %d excd %d
GW.005     ALWAYS   Bffrs: %d avail %d idle   fair %d low %d
GW.006     C-INFO    Pkt frm nt %d int %s/%d for uninit prt, disc
GW.007     C-INFO    Ip err %x nt %d int %s/%d
GW.008     U-INFO    Ip ovfl nt %d int %s/%d, disc
GW.009     UI-ERROR  Nt dwn ip rstrt nt %d int %s/%d
GW.010     UI-ERROR  Ip q len %d no ip buf nt %d int %s/%d
GW.011     U-INFO    Op err %x hst %wo nt %d int %s/%d
GW.012     U-INFO    Op err cnt excd hst %wo nt %d int %s/%d
GW.013     U-INFO    Rtrns cnt excd hst %wo nt %d int %s/%d
GW.014     UI-ERROR  Nt dwn op rstrt nt %d int %s/%d
GW.015     UI-ERROR  Nt dwn to hst %wo nt %d int %s/%d
GW.016     U-INFO    Op ovfl to hst %wo nt %d int %s/%d
GW.017     UE-ERROR  Intfc hdw mssng nt %d int %s/%d
GW.018     U-TRACE   Strt nt slf tst nt %d int %s/%d
GW.019     C-INFO    Slf tst nt %d int %s/%d
GW.020     U-TRACE   Nt pss slf tst nt %d int %s/%d
GW.021     UE-ERROR  Nt up nt %d int %s/%d
GW.022     U-TRACE   Nt fld slf tst nt %d int %s/%d
```

subsystems all
Lists all events in all subsystems.

trace-status
Displays information on the status of packet tracing, including configuration and run-time information.

Example:

```
list trace-status

------------------------- Configuration -----------------------------
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON  HD Shadowing:ON
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: TCP.013
Maximum Hours to HD Shadow:  1
```

Nodisplay

Use the **nodisplay** command to select and turn off messages displaying on the console.

Syntax:

nodisplay event. . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the displaying of a specified event (*subsystem.event#*).

group *groupname*
Suppresses the displaying of messages that were previously added to the specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the displaying of a range of messages for the specified subsystem.

Example:

```
nodisplay range gw 19 22
```

Suppresses the display of events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystemname*
Suppresses the displaying of messages associated with the specified subsystem.

Noremote

Use the **noremote** command to suppress the logging of events to a remote workstation based on event number, group, range of events, or subsystem.

Note: With the **noremote** command, there is usually no need to specify a *syslog_facility* and *syslog_level*, such as there is with the **remote** command. However, for **noremote subsystem** command, there exists the option of selectively suppressing specific message levels (for example, “error” only or “trace” only) rather than turning them all off. (If you do not specify any particular message level, “all” is assumed). Additionally, with the **noremote subsystem** command, you can set a *syslog_facility* and *syslog_level* for any remaining message levels that have not been turned off.

Syntax:

noremote event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the remote logging of messages for the specified event.

group *group.name*

Suppresses the remote logging of messages that were previously added to the specified group (*group.name*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the remote logging of a range of messages for the specified subsystem.

Example:

```
noremote range gw 19 22
```

Suppresses the remote logging of events gw.019, gw.020, gw.021, and gw.022

subsystem *subsystem.name [syslog_facility syslog_level]*

Suppresses the remote logging of messages associated with the specified subsystem (*subsystem.name*).

Example 1:

```
noremote subsystem tkr
```

Suppresses the remote logging of all “tkr” messages.

Example 2:

```
ELS config> noremote subsystem tkr info
ELS config> SYSLOG FACILITY[LOG_USER]?
ELS config> SYSLOG LEVEL[LOG_INFO]?
```

In this example, “LOG_USER” and “LOG_INFO” were the values last picked for subsystem TKR. The command specified turns off the remote logging for subsystem TKR only for messages coded for “info”. Because *syslog_facility* and *syslog_level* was not specified, the software prompts for *syslog_facility* and *syslog_level*. If you enter another value at the prompts, that value will replace *syslog_facility* and *syslog_level* for the remaining remote-logged messages for the TKR subsystem.

Use the **list all** or **list status** commands to display what you have set with the **noremote** and **remote** commands.

For more information about *syslog_facility* and *syslog_level* see “Remote” on page 173.

Notrace

Disables packet trace for the specified event/range/subsystem/group.

Syntax:

notrace event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the sending of packet trace data for the specified event#

group *groupname*
Suppresses the sending of packet trace data that was previously added to the specified group (groupname).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Disables the sending of packet trace data for a range of messages for the specified subsystem.

Example:

```
trace range gw 19 22
```

Suppresses the sending of packet trace data for events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystemname*
Suppresses the sending of packet trace data for the specified subsystem (subsystemname).

Notrap

Use the **notrap** command to select and turn off messages so that they are no longer sent to a network management workstation in SNMP traps.

Syntax:

notrap event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the sending of the specified message in an SNMP trap (*subsystem.event#*).

group *groupname*
Suppresses the sending of messages in SNMP traps that were previously added to the specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the sending of messages for the events in the specified range for the specified subsystem in SNMP traps.

Example:

```
notrap range gw 19 22
```

Suppresses the sending of messages for events gw.19, gw.20, gw.21, and gw.22 in SNMP traps.

subsystem *subsystemname*
Suppresses the sending of messages in SNMP traps that are associated with the specified subsystem.

Remote

Use the **remote** command to select the events to be logged to a remote workstation by event number, range of events, group, or subsystem.

Syntax:

remote event . . .
range . . .
group . . .
subsystem . . .

event *subsystem.event# syslog_facility syslog_level*
Causes the specified event to be logged remotely.

Syslog facility and level values are used by the syslog daemon in the remote workstation to determine where to log the messages. This value overrides the default values that are set with the **set facility** and **set level** commands.

syslog_facility
log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

syslog_level
log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug

These values do NOT have any particular association with any daemons on the IBM 8210. They are merely identifiers which are used by the syslog daemon on the remote workstation.

range *subsystemname first_event_number last_event_number syslog_facility syslog_level*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_numbe*r is the number of the last event of the specified event range.

Causes the events in the specified range for the specified subsystem to be remotely logged based on the *syslog_facility* and *syslog_level* values. See “the remote event command” on page 173.

Example:

```
remote range gw 19 22 log_user log_info
```

Causes the event gw.19, gw.20, gw.21, and gw.22 to be logged remotely on the *syslog_facility* value of log_user and the *syslog_level* value of log_info.

group *group.name syslog_facility syslog_level*

Allows events belonging to the specified group to be logged remotely based on the *syslog_facility* and *syslog_level* values. See “the remote event command” on page 173.

subsystem *subsystem.name message_level syslog_facility syslog_level*

Where *subsystem.name* is the name of the subsystem and *message_level* is the level of messages selected in the subsystem.

Causes the events within the specified *subsystem.name* whose *message_level* agrees with the specified *message_level* to be logged remotely at the files based on the *syslog_facility* and *syslog_level* values. See “the remote event command” on page 173.

Message_level is a value such as “ALL,” “ERROR,” “INFO,” or “TRACE” . See “Logging Level” on page 147. The value specified in the **remote** command must agree with the value as coded on the particular event within the subsystem, or that event within the subsystem will not be remotely logged.

Example:

```
remote subsystem TKR all log_user log_info
```

In the above example, all messages in subsystem TKR (“all” includes any messages coded for “error,” “info,” or “trace”) will be logged remotely based on log_user and log_info values at the remote host.

Use the **list all** or **list status** commands to display what you have set with the **noremote** and **remote** commands.

Set

Use the **set** command to set the maximum number of tags per second, the timestamp feature, or to set tracing options.

Syntax:

set

- pin . . .
- remote-logging . . .
- timestamp . . .
- trace . . .

pin *max_traps*

Use the **set pin** command to set the pin parameter to the maximum number of traps that can be sent on a per-second basis. Internally, the pin resets every tenth of a second. (One tenth of the number (*max_traps*) is sent every tenth of a second.)

remote-logging

Use the **set remote-logging** command to configure remote logging options. When these options are configured from the monitoring environment, the changes take effect immediately, and return to their previously configured settings when the device is rebooted.

Syntax:

set remote-logging on
off
facility . . .
level . . .
no-msgs
remote_ip_addr . . .
source_ip_addr ...
local_id

on Turns remote logging on. Remote logging is now enabled to allow any messages selected by the **remote** command to be actively logged.

off Turns remote logging off. All messages selected by the 'remote' command will be prevented from being logged.

facility

Specifies a value that, in combination with the *level* value, is used by the syslog daemon in the remote workstation to determine where to log messages. This value is used for all remotely-logged ELS messages unless you specify a different value for a particular ELS event, range, group, or subsystem with the **remote** command.

These are all possible syslog facility values:

log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

level Specifies a value that, in conjunction with the *facility* value, is used by the syslog daemon in the remote workstation to determine where

to log messages. This value is used for all remotely-logged ELS messages unless you specify a different value for a particular ELS event, range, group, or subsystem with the **remote** command.

These are all possible syslog level values:

log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug

no-msgs
Specifies the number of messages in the buffer for the remote log before log wraps.

remote_ip_addr
This is an ip address of the form xxx.xxx.xxx.xxx where xxx can be any integer 0 to 255. It represents the ip address of the remote host where the log files reside.

source_ip_addr
This is an ip address of the form xxx.xxx.xxx.xxx where xxx can be any integer 0 to 255.

You should use an IP address that is configured in the 8210 for easier identification when the IP address or the hostname is shown in the remotely-logged ELS message. You should also verify that this IP address is quickly resolved to a hostname by the name server, or at least that the name server responds quickly with "address not found."

To determine that the IP address resolves properly enter the **host** command on your workstation as shown:

```
workstation>host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

If the response takes more than 1 second, select an IP address that resolves more quickly.

local_id
This is any character string of up to 32 characters, which is included in the logged message at the remote file and can help identify which machine logged the message.

timestamp [timeofday or uptime or off]
Allows you to turn on message timestamping so that either the time of day or uptime (number of hours, minutes, and seconds, but no date, since the router was last initialized) appears next to each message. Set timestamp can also be turned off.

Use the **set timestamp** command to enable one of the following timestamp options.

timeofday
Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 24-hour day.

uptime
Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 100-hour cycle. After 100 hours of uptime, the uptime counter returns to zero to begin another 100-hour cycle.

off Turns off the ELS timestamp prefix.

trace Use the **set trace** command to configure tracing options. If you configure tracing options from the monitoring environment, the changes take effect immediately. They return to their previously configured settings when the device is rebooted.

Note: Tracing should be used only under the direction of trained support personnel. Tracing, especially when used with disk-shadowing enabled, uses device resources and can impact overall performance and throughput.

Syntax:

set trace
- decode
- default-bytes-per-pkt
- disk-shadowing
- max-bytes-per-pkt
- memory-trace-buffer-size
- off
- on
- reset
- stop-event
- wrap-mode

decode *off/on*
Turns packet decoding on or off. Packet decoding is not supported by all components.

default-bytes-per-pkt *bytes*
Sets the default number of bytes traced. This value is used if a value is not specified by the component doing the tracing.

disk-shadowing [[off or on] or record-size or time-limit or delete-file or max-file-size]
Turns disk shadowing on or off, sets the maximum trace file size, or sets the maximum time for disk-shadowing traces.

[off or on]
Turns disk shadowing on or off. If disk shadowing is enabled, trace records are copied to the hard disk. Once a traced record is copied to the hard disk, it can no longer be viewed from the monitoring.

Note: Disk shadowing should be set to OFF whenever the WRITE, TFTP software, RETRIEVE system dump, or COPY software commands are issued.

disk-shadowing delete-file
Deletes the trace file.

disk-shadowing max-file-size *Mbytes*
Sets the maximum file size for the trace file.

Valid Values: 1 Mbyte to 16 Mbytes

Default Value: 10 Mbytes

disk-shadowing record-size *bytes*
Sets the record size for trace file records:

Valid Values 1024, 2048, or 4096 bytes

Default 2048 bytes

Notes:

1. If a trace file already exists, “Cannot change Record Size without first deleting the existing Trace File” is displayed and record size is not changed.
2. If you configure a record size and a trace file already exists, the trace will use the record size of the existing file.

disk-shadowing time-limit *hours*
Sets the maximum time for disk-shadowing of traces:

Valid Values 1 - 72 hours

Default 24 hours

Note: Disk shadowing stops (tracing continues) after this time has elapsed. The actual time is reset to 0 when disk shadowing is turned on again.

max-bytes-per-pkt *bytes*
Sets the maximum number of bytes traced for each packet.

memory-trace-buffer-size *bytes*
Sets the size, in bytes, of the RAM trace buffer.

Valid Values: 0, ≥10,000

Default Value: 0

off Disables packet tracing.

on Enables packet tracing.

reset Clears the trace buffer and resets all associated counters.

stop-event *event id*
Stops tracing when an event (event id) occurs. Enter either an ELS event id (for example: TCP.013) or “None”. “None” is the default. Tracing stops only if the display of the particular ELS event is enabled.

When a stop-event occurs, an entry is written to the trace buffer. The **view** command for this trace entry will display “Tracing stopped due to ELS Event Id: TCP.013”.

After tracing stops due to a stop-event, you must re-enable tracing with the **set trace on** command. (A restart will also re-enable tracing if enabled from the `ELS Config>` prompt.)

wrap-mode [off or **on]**
Turns the trace buffer wrap mode on or off. If wrap mode is on and the trace buffer is full, previous trace records will be overwritten by new trace records as necessary to continue tracing.

Trace

Enables packet trace for the specified event/range/subsystem/group. When the **trace** command is used from the `ELS Config>` prompt, the changes become part of the configuration, and a reboot is required to activate the changes.

Syntax:

trace event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Causes the specified trace event (*subsystem.event#*) to be displayed on the system monitoring.

group *groupname*
Allows trace events that were previously added to the specified group to be displayed on the router monitoring.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the trace events in the specified range for the specified subsystem to be displayed on the system monitoring.

Example:

```
trace range gw 19 22
```

Causes the trace events gw.19, gw.20, gw.21, and gw.22 to be displayed on the system monitoring.

subsystem *subsystemname*
Allows trace events associated with the specified subsystem to be displayed on the router monitoring.

Trap

Use the **trap** command to select the message to be sent to the remote SNMP network management workstation. A remote SNMP network management workstation is an IP host in the network acting as an SNMP manager.

Syntax:

trap event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) to be sent to a network management workstation in an SNMP trap.

group *groupname*
Allows messages that were previously added to the specified group to be sent to a network management workstation in an SNMP trap.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem to be sent to a network management workstation in an SNMP trap.

Example:

```
trap range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 to be sent to a network management workstation in an SNMP trap.

subsystem *subsystemname*
Allows messages associated with the specified subsystem to be sent to a management station in an SNMP trap.

Note: Messages for the IP, ICMP, ARP and UDP subsystems cannot be sent in SNMP traps because these areas are or may be used in the process of sending the SNMP trap. This could lead to an infinite loop of traffic putting an undue strain on the router.

ELS Message Buffering Configuration Commands

Table 15 describes the commands available at the `ELS Config Advanced>` prompt.

Table 15. ELS Message Buffering Configuration Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
List	Displays the configuration settings for message buffering.
Log	Enables logging of selected messages to the message buffer.
Nolog	Turns off logging of selected messages to the message buffer.
Set	Sets the size of the message buffer, the wrapping mode, whether logging occurs, which event will end message buffering, and what the system does when message buffering is stopped by an event.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to list the ELS message buffering configuration.

Syntax:

list status

Example:

```
ELS Config Advanced> list status
---------------------------------Configuration-----------------------------------
Logging Status:    OFF    Wrap Mode:   ON  Logging Buffer Size:    8500   Kbytes
Stop-Event:    APPN.2          Stop-String:     netdn for  intf 6
Additional Stop-Action:  NONE
```

See “Set” on page 182 for a description of the commands that change the values in the display.

Log

Use the **log** command to select which messages will be logged to the message buffer.

Syntax:

log event
group
range
subsystem

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) to be logged to the message buffer.

group *groupname*
Allows messages that were previously added to the specified group to be logged to the message buffer.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem to be logged to the message buffer.

Example:

```
log range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 to be logged to the message buffer.

subsystem *subsystemname*
Allows messages associated with the specified subsystem to be logged to the message buffer.

Nolog

Use the **nolog** command to remove messages from the defined list of messages that are logged to the message buffer.

Syntax:

nolog event
group

range

subsystem

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) not to be logged to the message buffer.

group *groupname*
Allows messages that were previously added to the specified group not to be logged to the message buffer.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem not to be logged to the message buffer.

Example:

```
log range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 not to be logged to the message buffer.

subsystem *subsystemname*
Allows messages associated with the specified subsystem not to be logged to the message buffer.

Set

Use the **set** command to configure various ELS message buffering options.

Syntax:

set buffer-size *Kbytes*

logging [on or off]

stop action . . .

stop event *subsystem.event#*

stop string *text*

wrap on or off]

buffer-size *Kbytes*
Specifies the size, in kilobytes, of the message buffer that the system should allocate. The **mem** command displays this memory as “Never Alloc.” Setting this value too high could prevent the router from operating correctly after a reboot because of insufficient memory for protocols and features.

Valid values: 0 KB to 80% of the memory available on the router.

Default value: 0 (no message buffering)

Note: You must allocate a buffer with this command before you can set logging on.

logging [on or **off]**
Specifies whether message buffering will occur. This command will not take affect until you allocate a buffer using the **set buffer-size** command. The default is off.

stop action [appn-dump or **disk-offload**or **none** or **system-dump]**
Specifies the additional action the system takes when the "stop event" (and if specified, the "stop string") occurs. The actions are:

appn-dump
Dumps the APPN protocol, if it is active. The APPN dump will indicate that the dump was taken as the result of a stop action.

disk-offload
Writes a formatted version of the buffer to a file on the hard drive . If the file already exists, the new file replaces it. You can then use the **tftp file** monitoring command to send the file to a remote host.

none No other action is taken after logging stops.

system-dump
Dumps the entire system. The system dump will indicate that the dump was taken as the result of a stop action.

Default value: none

stop event [*subsystem.event#* or **none]**
Specifies the event (*subsystem.event#*) that stops logging. If you have specified a stop string, the text in the stop string must also match. When the stop event occurs:

1. The next five ELS messages are logged.
2. Logging stops.
3. The system performs the specified "stop action."

Logging remains stopped until the next time you issue the **set logging on** command or reboot the router.

If you do not specify the stop event when you enter the command, the system prompts you to enter the stop event. Specifying **none** disables the stop event function.

Default value: none

stop string *text* or **none**
Specifies the string to be used in conjunction with the "stop event" to stop logging. If you have not specified a stop event, the system ignores the "stop string."

Text can be any ASCII string up to 32 characters in length. If you do not specify *text* when you enter the command, the system will prompt you for the string. Entering **none** clears the "stop string."

Default value: none

wrap [on or **off]**
Specifies whether to stop the log when the buffer is full (off) or to log the new messages at the beginning of the buffer (on).

Default value: off

Entering and Exiting the ELS Operating Environment

The ELS monitoring environment (available from the GWCON process) is characterized by the ELS> prompt. Commands entered at this prompt modify the current ELS parameter settings. These commands are described “Chapter 14. Configuring and Monitoring the Event Logging System (ELS)” on page 165.

To enter the ELS monitoring environment from OPCON:

1. Enter the **console** command.

   ```
   * console
   ```

   The monitoring displays the GWCON prompt (+). If the prompt does not appear when you first enter GWCON, press **enter**.
2. At the GWCON prompt, enter the following command to access ELS:

   ```
   + event
   ```

   The monitoring displays the ELS monitoring prompt (ELS>). Now, you can enter ELS monitoring commands.

To leave the ELS monitoring environment, enter the **exit** command.

ELS Monitoring Commands

This section summarizes and then explains all the ELS monitoring commands. After accessing the ELS Monitoring environment, you can enter ELS monitoring commands at the ELS> prompt.

Table 16. ELS Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Advanced	Places you in the advanced configuration environment in which you can configure message buffering.
Clear	Resets to zero the counts of messages associated with specified events, groups, or subsystems.
Display	Enables message display on the console.
Exit	Exits the ELS console process and returns the user to GWCON.
List	Lists information on ELS settings and messages.
Nodisplay	Disables message display on the console.
Noremote	Disables remote logging to file at remote workstation.
Notrace	Disables trace event display on the console.
Notrap	Keeps messages from being sent out in SNMP traps to the network management workstation.
Packet-trace	Provides an enhanced central environment for setting and listing active packet tracing parameters.
Remote	Allows messages to be logged at a file on a remote workstation.
Remove	Frees up memory by erasing stored information.
Restore	Clears current settings and reloads initial ELS configuration.
Retrieve	Reloads the saved ELS configuration.
Save	Stores the current configuration.
Set	Sets the pin parameter and the timestamp feature.
Statistics	Displays available subsystems and pertinent statistics.
Trace	Enables trace event display on the console.

Table 16. ELS Monitoring Command Summary (continued)

Command	Function
Trap	Allows messages to be sent to a network management workstation in SNMP traps.
View	Allows viewing of traced packets.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Advanced

Use the **advanced** command to enter the advanced monitoring environment. In this environment you change message buffering operation.

Syntax:

advanced

Clear

Use the **clear** command to reset to zero the counts of the display, trace, trap, or remote commands as they relate to specific events, groups or subsystems.

Syntax:

clear event . . .
group . . .
subsystem . . .

event *subsystem. event#*
Resets the count of events to zero for displaying, trapping, tracing or remote logging of the specified event (*subsystem.event#*).

group *group.name*
Resets the count of events to zero for displaying, trapping, tracing or remote logging of the specified group (*group.name*).

subsystem *subsystem.name*
Resets the count of events to zero for displaying, trapping, tracing or remote logging of the specified subsystem (*subsystem.name*).

Display

Use the display command to enable the message display on the monitoring monitor for specific events.

Syntax:

display event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Displays messages for the specified event (subsystem.event#).

group *groupname*
Displays messages of a specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event in the specified event range.

Displays a range of messages for the specified subsystem.

Example:

```
display range gw 19 22
```

Displays events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystem.name*
Displays any messages associated with the specified subsystem (*logging level*). If you do not specify a logging level, all messages for that subsystem are turned on.

Files Trace TFTP

Use the **files trace tftp** command to retrieve trace files from the subdirectory associated with:

- The currently active bank (bank A or bank B on the hard disk)
- Bank A on the hard disk
- Bank B on the hard disk
- The trace file stored in the Network Subdirectory (if there is no active bank)

Syntax:

files trace tftp active-bank ...
bank-a ...
bank-b ...
net-subdir ...

You are prompted for the *remote server IP address* and the *remote path/file name*.

active-bank
Retrieves the traces file from the currently active bank

bank-a
Retrieves the trace file from bank A.

bank-b
Retrieves the trace file from bank B.

net-subdir
Retrieves the trace file stored in the Network Subdirectory (if there is no active bank).

List

Use the **list** command to get updated information regarding ELS settings and to get listings of selected messages.

Syntax:

list

- all
- active . . .
- event . . .
- groups . . .
- pin
- remote-log status
- subsystem . . .
- trace-status

all Lists all subsystems, defined groups, enabled subsystems, enabled events, and pins.

active *subsystem.name*
Displays the events that are active for a specific subsystem or have non-zero message counts.

Example:

```
list active ip
Event      Active  Count  Message

IP.007              2874  %I -> %I
IP.022                13  add nt %I int %I nt %n int %s/%d
IP.036              2874  rcv pkt prt %d frm %I
IP.058                23  del nt %I rt via %I nt %n int %s/%d
IP.068     D          37  routing cache cleared
D=Display on   T=Trap on   P=Packet Trace on   F=Filter on  R=Remote Logging on
A=Advanced on
```

If Remote logging is turned on, those events displayed as active for a subsystem will have an “R” next to their name.

event *subsystem.event#*
Displays the logging level, the message, and the count of the specified event.

Example:

```
list event ip.007

Level: p-TRACE
Message: source_ip_address -> destination_ip_address
Active:  Count: 84182
```

If Remote-logging had been activated for this event, and the *syslog_facility* and *syslog_level* values were log_daemon and log_crit, the last lines would look like:

```
Active:  R count:84182
Syslog Facility: log_daemon   Syslog Level: log_crit
```

groups *group.name*
Displays the user-defined group names.

pin Lists the current number of ELS event messages sent per second in SNMP traps. This is a threshold value that can be used to reduce the amount of SNMP trap traffic.

Example:

```
list pin

Pin: 100 events/second
```

remote-log status

Lists the current values of the remote logging options set in the **set remote-logging** command.

Example:

```
list r

Remote Logging is On
Source Ip Address = 192.9.200.8
Remote  Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_USER
Default Syslog Priority Level = LOG_INFO
Number of Messages in Remote Log = 256
Remote Logging Local ID =  SPHINX
```

subsystem *subsystem.name*

Lists event names, the total number of events that have occurred, and their descriptions.

Note: Although ELS supports all subsystems on the router, not all devices support all subsystems. See *ELS Messages* for a list of currently supported subsystems.

subsystem *subsystem.name*

Lists all events, logging levels, and messages for the specified subsystem.

Example:

```
list subsystem eth

Event      Level      Message
ETH.001    P-TRACE    brd rcv unkwn type packet_type source_Ethernet_address ->
                      destination_Ethernet_address nt network
ETH.002    UE-ERROR   rcv unkwn typ packet_type source_Ethernet_address ->
                      destination_Ethernet_address nt network
ETH.010    C-INFO     LLC unk SAP DSAP source_Ethernet_address ->
                      destination_Ethernet_address nt network
```

subsystem all

Lists all events, logging levels, and messages for every event that has occurred on the router.

trace-status

Displays information on the status of packet tracing, including configuration and run-time information.

Example:

```
list trace-status

------------------------ Configuration -----------------------------
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON  HD Shadowing:ON
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: TCP.013
Maximum Hours to HD Shadow:  1
----------------------- Run-time Status ---------------------------
Packets in RAM Trace Buffer:1   Free Trace Buffer Memory:99958
Trace Errors:0  First Packet:1  Last Packet:1
Trace Records Stored on HD:8  Trace Buffer File Size:16560
HD-Shadowing Time Exceeded? NO Elapsed Time:  0 hr,  0 min, 10 sec
Has Stop Trace Event Occurred? NO
```

- “Trace Status” in the LIST TRACE-STATUS display will indicate OFF when STOP-ON-EVENT action occurs.
- “HD Shadowing” in the LIST TRACE-STATUS display will indicate OFF when STOP-ON-EVENT action occurs or when Time Limit is exceeded.
- “Trace Buffer File Size” will display “<wrapped>” when a wraparound has occurred in the trace file.
- If disk-shadowing time limit is exceeded, but there has not been a trace record written since the time expired, then“ HD-Shadowing Time

Exceeded? NO <Next trace will turn it OFF>" will be displayed. When the next trace record has been written, then "HD-Shadowing Time Exceeded? YES" will be displayed.

ELS Config>**LIST TRACE** command under **talk 6** displays information similar to the following:

```
------------------------ Configuration -----------------------------
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON  HD Shadowing:ON
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: TCP.013
Maximum Hours to HD Shadow:  1
```

Nodisplay

Use the **nodisplay** command to select and turn off messages displaying on the console.

Syntax:

nodisplay event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the displaying of messages for the specified event.

group *group.name*
Suppresses the displaying of messages that were previously added to the specified group (*group.name*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the displaying of a range of messages for the specified subsystem.

Example:

```
nodisplay range gw 19 22
```

Suppresses the display of events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystem.name*
Suppresses the displaying of messages associated with the specified subsystem (*logging level*).

Noremote

Use the **noremote** command to select and turn off messages logging to a remote workstation.

Syntax:

noremote event . . .
group . . .

range . . .

subsystem . . .

event *subsystem.event#*
Suppresses the remote logging of messages for the specified event.

group *group.name*
Suppresses the remote logging of messages that were previously added to the specified group (*group.name*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the remote logging of a range of messages for the specified subsystem.

Example:

```
noremote range gw 19 22
```

Suppresses the remote logging of events gw.19, gw.20, gw.21, and g.22

subsystem *subsystem.name*
Suppresses the remote logging of messages associated with the specified subsystem (*logging level*).

Example:

```
noremote subsystem tkr
```

Note: With Noremote, there is no need to specify a Syslog Facility and Level, such as there is with Remote.

Use the **list event** and **list active** commands to verify what you set with the **remote** and **noremote** commands.

Notrace

Use the **notrace** command to stop display of selected trace events at the monitoring.

Syntax:

notrace event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the display of the specified tracing event.

group *groupname*
Suppresses the display of tracing events related to the specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Disables the sending of packet trace data for a range of messages for the specified subsystem.

Example:

```
notrace range gw 19 22
```

Suppresses the sending of packet trace data for events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystemname [logging-level]*

Suppresses the display of tracing events that are associated with the specified subsystem and logging level. If you do not specify a *logging-level* you suppress tracing for all logging levels for the subsystem.

Example:

```
notrace subsystem frl error

notrace subsystem frl
```

Notrap

Use the **notrap** command to select and turn off messages so that they are no longer sent to a network management workstation in SNMP traps.

Syntax:

notrap event. . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*

Suppresses the sending of the specified message in an SNMP trap (*subsystem.event#*).

group *groupname*

Suppresses the sending of messages in SNMP traps that were previously added to the specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the sending of messages for the events in the specified range for the specified subsystem in SNMP traps.

Example:

```
notrap range gw 19 22
```

Suppresses the sending of messages for events gw.19, gw.20, gw.21, and gw.22 in SNMP traps.

subsystem *subsystemname [logging-level]*

Suppresses the sending of messages in SNMP traps that are associated

with the specified subsystem and logging level. If you do not specify a *logging-level* you suppress trapping for all logging levels for the subsystem.

Example:

```
notrap subsystem eth error
```

Packet Trace

Use the **packet-trace** command to display/enable/disable packet tracing information for various subsystems.

Syntax:

packet-trace

Use the **Exit** command when you are finished using Packet Trace.

For complete command descriptions, see “Packet-trace Monitoring Commands” on page 204.

Remote

Use the **remote** command to select the events to be logged to a remote file by event number, range of events, group, or subsystem.

Syntax:

remote event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event# syslog_facility syslog_level*

Causes the specified event to be logged remotely.

Syslog facility and level values are used by the syslog daemon in the remote workstation to determine where to log the messages. This value overrides the default values that are set with the **set facility** and **set level** commands.

syslog_facility

log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

syslog_level

log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug

These values do NOT have any particular association with any daemons on the IBM 8210. They are merely identifiers which are used by the syslog daemon on the remote workstation.

Example:

```
remote event gw.019 log_user log_info
```

group *group.name syslog_facility syslog_level*

Allows events belonging to the specified group to be logged remotely based on the *syslog_facility* and *syslog_level* values. See "the remote event command" on page 192.

range *subsystemname first_event_number last_event_number syslog_facility syslog_level*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the events in the specified range for the specified subsystem to be remotely logged based on the *syslog_facility* and *syslog_level*. See "the remote event command" on page 192.

Example:

```
remote range gw 19 22 log_user log_info
```

Causes the event gw.19, gw.20, gw.21, and gw.22 to be logged remotely to the files specified by the *syslog_facility* value of log_user and the *syslog_level* value of log_info.

subsystem *subsystem.name message_level syslog_facility syslog_level*

Where *subsystem.name* is the name of the subsystem and *message_level* is the level of messages selected in the subsystem.

Causes the events within the specified *subsystem.name* whose *message_level* agrees with the specified *message_level* to be logged remotely based on the *syslog_facility* and *syslog_level*. See "the remote event command" on page 192.

Message_level is a value such as "ALL," "ERROR," "INFO," or "TRACE" . See "Logging Level" on page 147. The value specified in the **remote** command must agree with the value as coded on the particular event within the subsystem, or that event within the subsystem will not be remotely logged.

Example:

```
remote subsystem eth all log_user log_info
```

In the above example, all messages in subsystem TKR (“all” includes any messages coded for “error,” “info,” or “trace”) will be logged remotely to files specified by log_user and log_info at the remote host.

Use the **list event** and **list active** commands to verify what you set with the **remote** and **noremote** commands.

Remove

Use the **remove** command to free up memory by erasing stored information. If you have previously saved the current configuration with the **save** command, remove allows you to erase the saved configuration.

Syntax:

remove

Restore

Use the **restore** command to clear all current settings (except counters) and reload the initial ELS configuration. To retain the current settings, use the **save** command before restoring the initial configuration.

Syntax:

restore

Retrieve

Use the **retrieve** command to reload the saved ELS configuration. If you have previously saved the current configuration with the **save** command, use **retrieve** to reload it. **Retrieve** does not erase the saved configuration after it executes. To erase the saved configuration, use the **remove** command.

Syntax:

retrieve

Save

Use the **save** command to store the current configuration (except counters). **Save** does not affect the default configuration (the one you set with the configuration commands). Use **save** after modifying the configuration with the monitoring commands with the intention of saving this configuration over a restart. There can be only one saved configuration at a time. To reload the saved configuration, use the **retrieve** command.

Syntax:

save

Set

Use the **set** command to set the maximum number of traps per second, to set the timestamp feature, or to set the tracing options.

Syntax:

set pin . . .
remote-logging . . .
timestamp . . .
trace . . .

pin Use the **set pin** command to set the pin parameter to the maximum number of traps that can be sent on a per-second basis. Internally, the pin resets every tenth of a second. (One tenth of the number *max_traps* is sent every tenth of a second.)

remote-logging
Use the **set remote-logging** command to configure remote logging options. When these options are configured from the monitoring environment, the changes take effect immediately, and return to their previously configured settings when the device is rebooted.

Syntax:

set remote-logging on
off
facility . . .
level . . .
local_id
remote_ip_addr . . .
source_ip_addr ...

on Turns remote logging on. Remote logging is now enabled to allow any messages selected by the **remote** command to be actively logged.

off Turns remote logging off. All messages selected by the **remote** command will be prevented from being logged.

facility
Specifies a value that, in combination with the *level* value, is used by the syslog daemon in the remote workstation to determine where to log messages. This value is used for all remotely-logged ELS messages unless you specify a different value for a particular ELS event, range, group, or subsystem with the **remote** command.

These are all possible syslog facility values:

log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user

log_uucp
log_local0-7

level Specifies a value that, in conjunction with the *facility* value, is used by the syslog daemon in the remote workstation to determine where to log messages. This value is used for all remotely-logged ELS messages unless you specify a different value for a particular ELS event, range, group, or subsystem with the **remote** command.

These are all possible syslog level values:

log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug

local_id
Specifies a 1-32 character identifier that appears in the remote logging message that you can use to identify which machine logged a particular message.

remote_ip_addr
This is an IP address of the remote host where the log files reside.

source_ip_addr
Specifies the IP address of the machine that originated the message that is being remotely-logged.

You should use an IP address that is configured in the 8210 for easier identification when the IP address or the hostname is shown in the remotely-logged ELS message. You should also verify that this IP address is quickly resolved to a hostname by the name server, or at least that the name server responds quickly with "address not found."

To determine that the IP address resolves properly enter the **host** command on your workstation as shown:

```
workstation>host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

If the response takes more than 1 second, select an IP address that resolves more quickly.

timestamp
Allows you to turn on message timestamping so that either the time of day or uptime (number of hours, minutes, and seconds, but no date, since the router was last initialized) appears next to each message, or to turn off message timestamping.

Note: If you turn on timestamping, you must remember to go back into the CONFIG process and set the router's date and time using the time command. Otherwise, all messages will come out with 00:00:00, or negative numbers in the hours, minutes, and/or seconds, for example 00:-4:-5.

Use the **set timestamp** command to enable one of the following timestamp options:

timeofday
Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 24-hour day.

uptime
Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 100-hour cycle of uptime for the router. After 100 hours of uptime, the uptime counter returns to zero to begin another 100-hour cycle.

off Turns off the ELS timestamp prefix.

Syntax:

set timestamp [timeofday or uptime or off]

trace Use the **set trace** command to configure tracing options. When tracing options are configured from the monitoring environment, the changes take effect immediately, and return to their previously configured settings when the device is rebooted.

Syntax:

set trace decode . . .
default-bytes-per-pkt . . .
disk-shadowing . . .
max-bytes-per-pkt . . .
memory-trace-buffer-size . . .
off
on
reset
stop-event . . .
wrap-mode . . .

decode . . .
Sets packet decode options. Packet decoding is not supported by all components.

exclude
Excludes the specified frame type for decode. The possible frame types for exclusion are:

lecontrol
LE Control

ip IP

arp ARP

ipx IPX

netbios
NetBIOS

bpdu BPDU

appletalk
AppleTalk

aarp AppleTalk ARP

hex Turns off printing of hexadecimal frame data.

summary
Turns off printing of a one-line summary decode. A complete decode is printed.

all Excludes all packet types from the trace. No frame types are decoded.

none Excludes no packet types from the trace. *exlcude all*.

include
Includes the specified frame type for decode. The possible frame types for inclusion are:

lecontrol
LE Control

ip IP

arp ARP

ipx IPX

netbios
NetBIOS

bpdu BPDU

appletalk
AppleTalk

aarp AppleTalk ARP

hex Turns on printing of hexadecimal frame data.

summary
Turns on printing of a one-line summary decode. A complete decode is not printed.

all Includes all packet types in the trace.

none Includes no packet types in the trace. This is the opposite of *include all*.

off Sets decoding off.

on Sets decoding on.

Note: The default setting is to print complete decode output for all frame types. Use the **list trace-status** command to see the current decode settings. See page 188.

default-bytes-per-pkt *bytes*
Sets the default number of bytes traced. This value is used if a value is not specified by the component doing the tracing.

disk-shadowing [[off or on] or [delete-file or *record-size* **or** *time-limit*]]
Turns disk shadowing on or off, sets the maximum trace file size, or sets the maximum time for disk-shadowing traces.

[off or on]

Turns disk shadowing on or off. If disk shadowing is enabled, trace records are copied to the hard disk. Once a traced record is copied to the hard disk, it can no longer be viewed from the monitoring.

Note: Disk shadowing should be set to OFF whenever the WRITE, TFTP software, RETRIEVE system dump, or COPY software commands are issued.

Turns disk shadowing on or off and sets the maximum trace file size. If disk shadowing is enabled, trace records are copied to the hard disk. Once a traced record is copied to the hard disk, it is no longer viewable through the monitoring.

record-size *bytes*

Sets the record size for trace file records:

Valid Values: 1024, 2048, or 4096 bytes

Default: 2048 bytes

Notes:

1. If a trace file already exists, “Cannot change Record Size without first deleting the existing Trace File” is displayed and record size is not changed.
2. If you configure a record size and a trace file already exists, the trace will use the record size of the existing file.

delete-file

Deletes the trace file (in the subdirectory associated with the active bank only).

Note: If disk shadowing is ON when the command is issued, “ Disk-shadowing must be set to OFF before trace file can be deleted” is displayed and the file is not deleted.

time-limit *hours*

Sets the maximum time for disk-shadowing of traces:

Valid Values:
1 - 72 hours:

Default
24 hours

Note: Disk shadowing stops (tracing continues) after this time has elapsed. The actual time is reset to 0 when disk shadowing is turned on again.

max-bytes-per-pkt *bytes*

Sets the maximum number of bytes traced for each packet.

memory-trace-buffer-size *bytes*

Sets the size, in bytes, of the RAM trace buffer.

Valid Values: 0, ≥10,000

Default Value: 0

off Disables packet tracing.

on Enables packet tracing.

reset Clears the trace buffer and resets all associated counters.

stop-event *event id*
Stops tracing when an event (event id) occurs. Enter either an ELS event id (for example: TCP.013) or “None”. “None” is the default. Tracing stops only if the display of the particular ELS event is enabled.

When a stop-event occurs, an entry is written to the trace buffer. The **view** command for this trace entry will display “Tracing stopped due to ELS Event Id: TCP.013”.

After tracing stops due to a stop-event, you must re-enable tracing with the **set trace on** command. (A restart will also re-enable tracing if enabled from the `ELS Config>` prompt.)

Example:

```
set trace stop-event TCP.013
```

wrap-mode *off/on*
Turns the trace buffer wrap mode on or off. When wrap mode is enabled and the trace buffer is full, previous trace records will be overwritten by new trace records as necessary to continue tracing.

Statistics

Use the **statistics** command to display a list of all of the available subsystems and their statistics.

Note: The following example may not match your display exactly. The output of the command depends on the version and release of the installed software.

Syntax:

statistics

Example:

```
statistics

Subsys  Vector  Exist   String  Active    Heap

  GW     105     101      3411     0         0
 FLT      20       7       184     0         0
 BRS      50       5       201     0         0
 ARP     150     142      7030     0         0
  IP     100     100      2463     2        20
ICMP      30      21       529     0         0
 TCP      60      57      2420     0         0
 UDP      10       6       179     0         0
 BTP      40      13       695     0         0
 RIP      30      22       474     0         0
OSPF      80      73      2859     0         0
MSPF      40      17       593     0         0
TFTP      35      29       819     0         0
SNMP      30      28       821     0         0
 DVM      30      21       589     0         0
  DN     140     115      5842     0         0
  XN      35      21       780     0         0
 IPX     110     110      4705     0         0
CLNP      80      58      1763     0         0
ESIS      40      24       716     0         0
ISIS      80      58      2422     0         0
DNAV      50      26      1314     0         0
```

```
 AP2      80      70      1755     0         0
ZIP2      60      51      1859     0         0
R2MP      50      38      1185     0         0
 VIN      90      79      3159     0         0
 SRT     120      94      5040     0         0
 STP      60      32      1590     0         0
  BR      50      30      1616     0         0
SRLY      30      28      1409     0         0
 ETH      60      47      1098     0         0
  SL      50      35       584     0         0
 TKR      60      45      2031     0         0
 X25      70      53      1909     0         0
FDDI      30      27      1155     0         0
SDLC     100      95      4263     0         0
 FRL     130      97      6068     0         0
 PPP     190     186      6394     0         0
X251      50      16       546     0         0
X252      50      34       996     0         0
X253      50      42      1649     0         0
ISDN      50      43      1994     0         0
IPPN      20       4       132     0         0
 WRS      40      33      1938     0         0
 LNM      70      60      3137     0         0
 LLC     170     168      9840     0         0
 BGP      80      74      2477     0         0
 MCF      15       9       244     0         0

 V25B     30      28      1058     0         0

 COMP     80      26      1050     0         0
 NBS     100      50      3029     0         0
 ATM     300     216     10808     0         0
 LEC     200     174      7258     0         0
APPN     100      28       467     0         0
ILMI     150      23       487     0         0
SAAL      30      26       621     0         0
 SVC      30      26       465     0         0
 LES     400     361     22333     0         0
LECS     150     145      5666     0         0

EVLOG      1       1       105     0         0
 NOT      25      15       508     0         0
NHRP     250     211      8193     0         0
 XTP      64      58      2271     0         0
 ESC     150      67      3122     0         0
 LCS      40      22       858     0         0
 LSA      70      61      3506     0         0
 MPC     130      30      1677     3        44
SCSP      40      34      1234     0         0
ALLC      50      36      1842     0         0
 NDR      50      38      1150     0         0
 MLP     100      93      4006     0         0
 SEC      50      30       688     0         0
ENCR     100       4       194     0         0
  PM      25       6       120     0         0
 DGW      20       9       238     0         0
QLLC      55      54      2411     0         0

Total   6490    4942    215805     5        64

Maximum:7976 vector, 155 subsystem
Memory:71784/620 vector+ 81256/217714 data+ 64 heap=371438Subsys
```

Subsys
Name of subsystem

Vector
Maximum size of subsystem

Exist Number of events defined in this subsystem

String Number of bytes used for message storage in this subsystem

Active Number of active (displayed, trapped, or counted) events in the subsystem

Heap Dynamic memory in use by subsystem

Trace

Use the **trace** command to select the trace events to be displayed on the system monitoring. This command provides function that is similar to the **packet trace** command described in “Packet-trace Monitoring Commands” on page 204.

Syntax:

trace event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Causes the specified trace event (*subsystem.event#*) to be displayed on the system monitoring.

group *groupname*
Allows trace events that were previously added to the specified group to be displayed on the router monitoring.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_numbe*r is the number of the last event of the specified event range.

Causes the trace events in the specified range for the specified subsystem to be displayed on the system monitoring.

Example:

```
trace range gw 19 22
```

Causes the trace events gw.19, gw.20, gw.21, and gw.22 to be displayed on the system monitoring.

subsystem *subsystemname*
Allows trace events associated with the specified subsystem to be displayed on the router monitoring.

Trap

Use the **trap** command to select the message to be sent to the remote SNMP network management workstation. A remote SNMP network management workstation is an IP host in the network acting as an SNMP manager.

Syntax:

trap event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) to be sent to a network management workstation in an SNMP trap.

group *groupname*
Allows messages that were previously added to the specified group to be sent to a network management workstation in an SNMP trap.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem to be sent to a network management workstation in an SNMP trap.

Example:

```
trap range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 to be sent to a network management workstation in an SNMP trap.

subsystem *subsystemname*
Allows messages associated with the specified subsystem to be sent to a management station in an SNMP trap.

Note: Messages for the IP, ICMP, ARP and UDP subsystems cannot be sent in SNMP traps because these areas are or may be used in the process of sending the SNMP trap. This could lead to an infinite loop of traffic putting an undue strain on the router.

View

Use the **view** command to view traced packets.

Syntax:

view current
first
jump
last
next
prev
search ...

current
Displays the current trace packet. If the current packet is not valid, the first packet in the trace buffer is displayed.

first Displays the first traced packet in the trace buffer.

jump *n*
Displays the traced packet *n* packets ahead of or behind the current packet.

last Displays the last traced packet in the trace buffer.

next Displays the next traced packet.

prev Displays the previous traced packet.

search
Displays the next traced packet that contains the specified information. You can specify the search information by:

- Hexadecimal string
- IP address
- ASCII text

Packet-trace Monitoring Commands

This section describes the Packet-trace Monitoring commands. After accessing the Packet-trace Monitoring environment, you can enter Packet-trace Monitoring commands at the `ELS Packet Trace>` prompt.

Table 17. Packet Trace Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Off	Disables packet tracing.
On	Enables packet tracing. Prompts for memory trace buffer size if not previously set.
Reset	Clears the trace buffer and resets all associated counters.
Set	Configures tracing options.
Subsystems	Activates tracing for the subsystems that support packet tracing, or displays a summary.
Trace-status	Displays information on the status of packet tracing, including configuration and run-time.
View	Provides View Captured Packet Trace Buffers Console
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Off

Use the **off** command to disable packet tracing.

Syntax:

off

On

Use the **on** command to enable packet tracing.

Syntax:

on

Reset

Use the **reset** command to clear the trace buffer and reset all associated counters.

Syntax:

reset

Set

Use the **set** command to configure tracing options.

Syntax:

set	decode
	default-bytes-per-pkt
	disk-shadowing
	max-bytes-per-pkt
	memory-trace-buffer-size
	stop-event
	wrap-mode
	exit

For an explanation of the `set` command, see page 197.

Subsystems

Use the **subsystems** command to activate tracing for the subsystems that support packet tracing, or to display a summary.

Syntax:

subsystems	atm
	fddi
	ilec
	lec
	lecs
	les-bus
	se
	summary

Example:

```
subsystems atm
Network number? 0
ATM Interface is selected
on | off | list [list]? on
Note that SVC  uses VPI = 0, VCI = 5
and ILMI uses VPI = 0, VCI = 16
Beginning of VPI range [0]?
End of VPI range [0]?
Beginning of VCI range [0]? 16
End of VCI range [0]? 16
Tracing event ATM.88: ATM frames
```

Example:

```
subsystems lec
Network number? 1
ATM Emulated LAN is selected
on | off | list [list]? on
Trace which types of frames (data, control, both) [both]?
Tracing event LEC.11: data frames over ATM Forum LEC: interface 1
Tracing event LEC.12: control frames over ATM Forum LEC: interface 1
Note that if the user DISABLEs and TESTs this LEC interface,
```

```
the LEC trace settings from Talk 6 Config will take effect.

MAC Address packet filtering can be enabled under the LEC net
using the 'trace mac-address' command.
```

Example:

```
subsystems lecs
LECS Environment
on | off | list [list]? on
LECS modified
LECS modified
Tracing event LECS.128: control frames
(To trace a subset of LEC's, use the SET TRACE VALUE and
 SET TRACE MASK commands while using the LECS monitoring.)
```

Example:

```
subsystems les-bus
LES-BUS Environment
  (  1) ELAN0
  (  2) ELANE
  (  3) (Select All)
Choice of LES/BUS [1]? 2
on | off | list [list]? on
LES/BUS: 'ELANE' : parameter successfully set
LES/BUS: 'ELANE' : parameter successfully set
Trace which types of frames (data, control, both) [both]? data
Tracing event LES.257: data frames
(To trace a subset of LEC's, use the SET TRACE VALUE and
SET TRACE MASK commands while WORK'ing with the LES-BUS.)
```

Example:

```
subsystems summary
Subsystems Being Traced

ATM        net number = 0, VPI Range:     0 -     0
                           VCI Range:    16 -    16
LEC        net number = 1
LECS
LESBUS     elan name = ELAN0
LESBUS     elan name = ELANE
```

Trace-Status

Use the **trace-status** command to get updated information regarding packet trace.

Syntax:

trace-status

Example:

```
trace-status
------------------------ Configuration -----------------------------
Trace Status:OFF  Wrap Mode:OFF  Decode Packets:OFF  HD Shadowing:OFF
RAM Trace Buffer Size:0  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: None
Maximum Hours to HD Shadow:  24
----------------------- Run-time Status ---------------------------
Packets in RAM Trace Buffer:0   Free Trace Buffer Memory:0
Trace Errors:0  First Packet:0  Last Packet:0
Trace Records Stored on HD:0  Trace Buffer File Size:0
HD-Shadowing Time Exceeded? NO
Has Stop Trace Event Occurred? NO
```

View

Use the **view** command to enter the View Captured Packet Trace Buffers Monitoring.

For an explanation of the **view** commands, see “View” on page 203.

Syntax:

view current
first
jump
last
next
prev
search
exit

ELS Message Buffering Monitoring Commands

Table 18 describes the commands available at the `ELS Config Advanced>` prompt.

Table 18. ELS Message Buffering Monitoring Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Flush	Clears the message buffer and turns off logging to the message buffer.
List	Displays the operational settings for message buffering.
Log	Enables logging of selected messages to the message buffer.
Nolog	Turns off logging of selected messages to the message buffer.
Read-file	Reads a formatted message buffer from a file and displays it on the console.
Set	Sets the size of the message buffer, the wrapping mode, whether logging occurs, which event will end message buffering, and what the system does when message buffering is stopped by an event.
Tftp	Sends the ELS message buffer to a file at a remote host.
View	Displays all or a specific number of messages in the message buffer. You can also control how the messages scroll off the screen.
Write-buffer	Writes the ELS message buffer to the hard drive . The buffer is formatted before it is written. The file name on the hard drive is always ELSADV.LOG.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Flush

Use the **flush** command to set logging off, clear the messages from the buffer, and release the buffer memory for other use by the system.

Syntax:

flush buffer

List

Use the **list** command to list the ELS message buffering configuration.

Syntax:

list status

Example:

```
ELS Advanced> list status
-----------------------------------Configuration--------------------------------
Logging Status:    OFF       Wrap Mode:   ON    Logging Buffer Size:    8500 Kytes
Stop-Event:    APPN.2          Stop-String:     netdn for  intf 6
Additional Stop-Action:  APPN DUMP
-----------------------------------Run-Time Status------------------------------
Has Stop Condition Occurred ?     YES       Messages currently in buffer:         1222
```

See “Set” on page 209 for a description of the commands that change the values in the display.

Log

Use the **log** command to select which messages will be logged to the message buffer.

Syntax:

log event
group
range
subsystem

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) to be logged to the message buffer.

group *groupname*
Allows messages that were previously added to the specified group to be logged to the message buffer.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem to be logged to the message buffer.

Example:

```
log range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 to be logged to the message buffer.

subsystem *subsystemname*
Allows messages associated with the specified subsystem to be logged to the message buffer.

Nolog

Use the **nolog** command to remove messages from the defined list of messages that are logged to the message buffer.

Syntax:

nolog event
group
range
subsystem

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) not to be logged to the message buffer.

group *groupname*
Allows messages that were previously added to the specified group not to be logged to the message buffer.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem not to be logged to the message buffer.

Example:

```
log range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 not to be logged to the message buffer.

subsystem *subsystemname*
Allows messages associated with the specified subsystem not to be logged to the message buffer.

Read-file

Use the **read-file** command to read formatted ELS messages from a file on the hard drive , `ELSADV.LOG`, created by the **write-buffer** command.

Note: If you enter this command and a hard drive is not available, you will receive a message indicating the drive is unavailable.

Syntax:

read-file

Set

Use the **set** command to change configured ELS message buffering options.

Syntax:

set logging [on or off]
stop action . . .

stop event *subsystem.event#*

stop string *text*

wrap [on or off]

logging [on or **off]**
Specifies whether message buffering will occur. This command will not take affect until you allocate a buffer using the **set buffer-size** command. The default is off.

stop action [appn-dump or **disk-offload**or **none** or **system-dump]**
Specifies the additional action the system takes when the "stop event" (and if specified, the "stop string") occurs. The actions are:

appn-dump
Dumps the APPN protocol, if it is active. The APPN dump will indicate that the dump was taken as the result of a stop action.

disk-offload
Writes a formatted version of the buffer to a file on the hard drive . If the file already exists, the new file replaces it. You can then use the **tftp file** monitoring command to send the file to a remote host.

none No other action is taken after logging stops.

system-dump
Dumps the entire system. The system dump will indicate that the dump was taken as the result of a stop action.

Default value: none

stop event [*subsystem.event#* or **none]**
Specifies the event (*subsystem.event#*) that stops logging. If you have specified a stop string, the text in the stop string must also match. When the stop event occurs:

1. The next five ELS messages are logged.
2. Logging stops.
3. The system performs the specified "stop action."

Logging remains stopped until the next time you issue the **set logging on** command or the router reboots.

If you do not specify the stop event when you enter the command, the system prompts you to enter the stop event. Specifying **none** disables the stop event function.

Default value: none

stop string *text* or **none**
Specifies the string to be used in conjunction with the "stop event" to stop logging. If you have not specified a stop event, the system ignores the "stop string."

Text can be any ASCII string up to 32 characters in length. If you do not specify *text* when you enter the command, the system will prompt you for the string. Entering **none** clears the "stop string."

Default value: none

wrap [on or **off]**
Specifies whether to stop the log when the buffer is full (off) or to log the new messages at the beginning of the buffer (on).

Default value: off

Tftp

Use the **tftp** command to send the ELS message buffer to a remote host as a formatted file.

Syntax:

tftp buffer [formatted] *dest_ip_address dest_filename*

file *dest_ip_address dest_filename*

buffer [formatted] *dest_ip_address dest_filename*
Specifies that the ELS message buffer is to be sent to the remote host indicated by *dest_ip_address* as file *dest_filename.* The buffer can be either formatted.

View

Use the **view** command to view all of the messages or a specific number of messages in the message buffer.

Syntax:

view all [scroll/noscroll]

last [scroll/noscroll *number*]

all *scroll/noscroll*
Displays all of the messages in the message buffer.

[scroll]
Specifies that the screen pauses until you hit the spacebar.

Note: If you are displaying a large number of messages, specify scroll so you do not miss any critical messages.

noscroll
Specifies that the messages will scroll off the screen if the number of messages exceeds the screen length.

last *scroll/noscroll number*
Display the last *number* messages in the message buffer.

[scroll]
Specifies that the screen pauses after displaying a full screen of messages and waits for the user to hit the space bar to get the next screen.

Note: If you are displaying a large number of messages, specify scroll so you do not miss any critical messages.

noscroll
Specifies that the messages will continuously scroll off the screen with no scroll control until either all messages in the buffer (or the last number of messages requested) have been displayed.

number
Specify a number from 1 to the total number of messages in the message buffer. To display the total number of messages in the buffer, use the **list status** monitoring command.

Write-buffer

Use the **write-buffer** command to write formatted ELS messages to the hard drive .

Note: If you enter this command and a hard drive is not available, you will receive a message indicating the drive is unavailable.

Syntax:

write-buffer

Chapter 15. Configuring and Monitoring Performance

This chapter describes how to use the Performance configuration and monitor operating commands and includes the following sections:

- "Performance Overview"
- "Performance Reporting Accuracy"
- "Accessing the Performance Configuration Environment"
- "Performance Configuration Commands" on page 214
- "Accessing the Performance Monitoring Environment" on page 215
- "Performance Monitoring Commands" on page 215

Performance Overview

Configuring performance allows you to monitor your CPU load. In the idle (non-work load) state, performance reflects operations that the router continuously performs as a part of managing external interfaces. The CPU load registered in the idle state is dependent upon:

- Number of protocols running.
- Number of interfaces/cards installed.
- Type of interfaces installed.

The performance function can be used as a tool for trend analysis, bottleneck evaluation, and capacity planning. By collecting the CPU utilization information on the router, a network manager can monitor:

- CPU load versus time of day.
- CPU load versus location of the router in the network.
- CPU load versus traffic throughput.
- CPU load versus user load

Performance Reporting Accuracy

If you request a performance analysis when the 8210 first comes online, you will see values that reflect an initialization state that has little or no network traffic, so it is of little use in helping to balance your network load.

It is best to use performance reports that are generated under normal loads after approximately 2 minutes of operation.

Accessing the Performance Configuration Environment

Use the following procedure to access the Performance monitor configuration process.

1. At the OPCON prompt, enter **talk 6**. (For more detail on this command, see "What is CONFIG?" on page 85.) For example:

```
* talk 6
Config>
```

© Copyright IBM Corp. 1996, 1998

After you enter the **talk 6** command, the CONFIG prompt (`Config>`) displays on the terminal. If the prompt does not appear when you first enter configuration, press **enter** again.

2. At the CONFIG prompt, enter the **perf** command to get to the `PERF Config>` prompt.

Performance Configuration Commands

To configure Performance, enter the commands at the `PERF Config>` prompt.

Table 19. PERF Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Disable	Disables the collection of CPU utilization statistics or `Talk 2` ELS monitor output.
Enable	Enables the collection of CPU utilization statistics or `Talk 2` ELS monitor output.
List	Lists the configuration.
Set	Sets the reporting period.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Disable

Use the **disable** command to disable collection of CPU utilization statistics and disable the `talk 2` ELS monitor output.

Syntax:

disable cpu statistics

t2 output

Enable

Use the **enable** command to enable collection of CPU utilization statistics and enable the `talk 2` ELS monitor output.

Syntax:

enable cpu statistics

t2 output

List

Use the **list** command to display the performance monitor configuration.

Syntax:

list

Set

Use the **set** command to set the reporting period.

Syntax:

set *time*

time Specifies the short window time.

Valid Values: 2 - 30 seconds

Default Value: 2

Accessing the Performance Monitoring Environment

Use the following procedure to access the Performance monitoring commands. This process gives you access to the Performance *monitoring* process.

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, see "Chapter 11. The Operating/Monitoring Process (GWCON - Talk 5) and Commands" on page 129.) For example:

   ```
   * talk 5
   +
   ```

   After you enter the **talk 5** command, the GWCON prompt (+) displays on the terminal. If the prompt does not appear when you first enter configuration, press **enter** again.

2. At the + prompt, enter the **perf** command to get you to the `PERF Console>` prompt.

   Example:

   ```
   + perf
   PERF Console>
   ```

Performance Monitoring Commands

This section describes the Performance monitoring commands.

Table 20. PERF Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Clear	Clear the CPU utilization high water statistics and resets the reporting period to a new cycle.
Disable	Disables the collection of CPU utilization statistics or `Talk 2` ELS monitor output.
Enable	Enables the collection of CPU utilization statistics or `Talk 2` ELS monitor output.
List	Lists the configuration.
Report	Displays a report of performance statistics.
Set	Sets the reporting period.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

Disable

Use the **disable** command to disable collection of CPU utilization statistics and disable the `talk 2` ELS monitor output.

Syntax:

disable	cpu statistics
	t2 output

Enable

Use the **enable** command to enable collection of CPU utilization statistics and enable the `talk 2` ELS monitor output.

Syntax:

enable	cpu statistics
	t2 output

List

Use the **list** command to display the performance monitor configuration.

Syntax:

list

Report

Use the **report** command to display performance monitor statistics.

Syntax:

report

Example:

```
PERF Console>report
------------------------------------------------------------
KEY:  SW = Short Window = 9 seconds
KEY:  LW = Long Window =  9.0 minutes  (60 x SW)

  CPU UTIL :   Most recent SW                    = 38%
               Most recent LW                    = 33%
               Highest for all SW's              = 92%
               Highest for all LW's              = 52%
               % of time cpu util (SW) was > 60%  = 16%
               % of time cpu util (SW) was > 70%  = 15%
               % of time cpu util (SW) was > 80%  = 1%
               % of time cpu util (SW) was > 90%  = 0%
               % of time cpu util (SW) was > 95%  = 0%
------------------------------------------------------------
```

Set

Use the **set** command to set the reporting period.

Syntax:

set *time*

time Specifies the short window time.

Valid Values: 2 - 30 seconds

Default Value: 2

Performance Monitoring Commands (Talk 5)

Chapter 16. Using FDDI

This chapter describes how to set software-configurable information for the Fiber Distributed Data Interface (FDDI) in the router.

This chapter contains the following sections:

- "Fiber Distributed Data Interface (FDDI) Overview"

Fiber Distributed Data Interface (FDDI) Overview

Fiber Distributed Data Interface (FDDI) is described by the ANSI X3T9.5 and ISO 9314 committees as a dual counter-rotating ring that operates at a defined speed of 100 Mbps.

In many ways, FDDI is similar to the IEEE 802.5 token-ring, although there are differences, some of which are described in "Differences Between FDDI and Token-Ring" on page 220.

Token-Passing Ring Network

FDDI is defined as a token-passing protocol. Each station has the chance to transmit data when a token passes. A station can decide how many frames it will transmit using an algorithm that permits "bandwidth" allocating.

FDDI also allows a station to transmit many frames without releasing the token in a way that is similar to the IEEE 802.5 token-ring standard.

An FDDI ring network consists of a set of stations/devices connected as a serial string of stations/devices and transmission media to form a physically closed loop. Information is transmitted sequentially as a stream of suitably encoded signals from one active station/device to the next active one.

Each station/device generally regenerates and repeats each token and can serve as the means of attaching one or more stations/devices to the network.

Primary and Secondary Rings

FDDI defines two rings:

- The *primary ring*, which is similar to the main ring path in a token-ring network.
- The *secondary ring*, which is similar to the backup ring path in a token-ring network.

Each ring path consists of two fibers, each fiber transmitting one signal; one is pushed and one is pulled in a device. Each fiber is equivalent to a pair of copper conductors. The physical approach in terms of fiber optics is similar to physical fiber optic token-ring paths.

Attachment of Devices

FDDI permits many attachment units:

- Stations or devices

© Copyright IBM Corp. 1996, 1998

- Concentrators
- Bridges

These units can be attached to FDDI networks in various ways, similar to those for token-ring networks.

Differences Between FDDI and Token-Ring

The main differences between FDDI and token-ring techniques are:

- A device can be attached directly to rings without a concentrator, such as a multi-station access unit (MSAU) on a token ring.
- A device can be attached to either or both of the primary and secondary rings.

FDDI defines two device classes, A and B, to differentiate between devices that attach to one ring or both rings, as described in the next section.

Device Classes A and B

FDDI defines two device classes:

- A **Class A** device attaches to both rings directly.

  It can be a station, called a *Class A station* or *Dual Access Station (DAS)*, or it can be a Concentrator, called a *Dual Access Concentrator (DAC)*
- A **Class B** device attaches to only one of the rings directly or through a concentrator.

  It can be a station, called a *Class B station* or *Single Access Station (SAS)*, or it can be a Concentrator, called a *Single Access Concentrator (SAC)*

FDDI Network Diagram

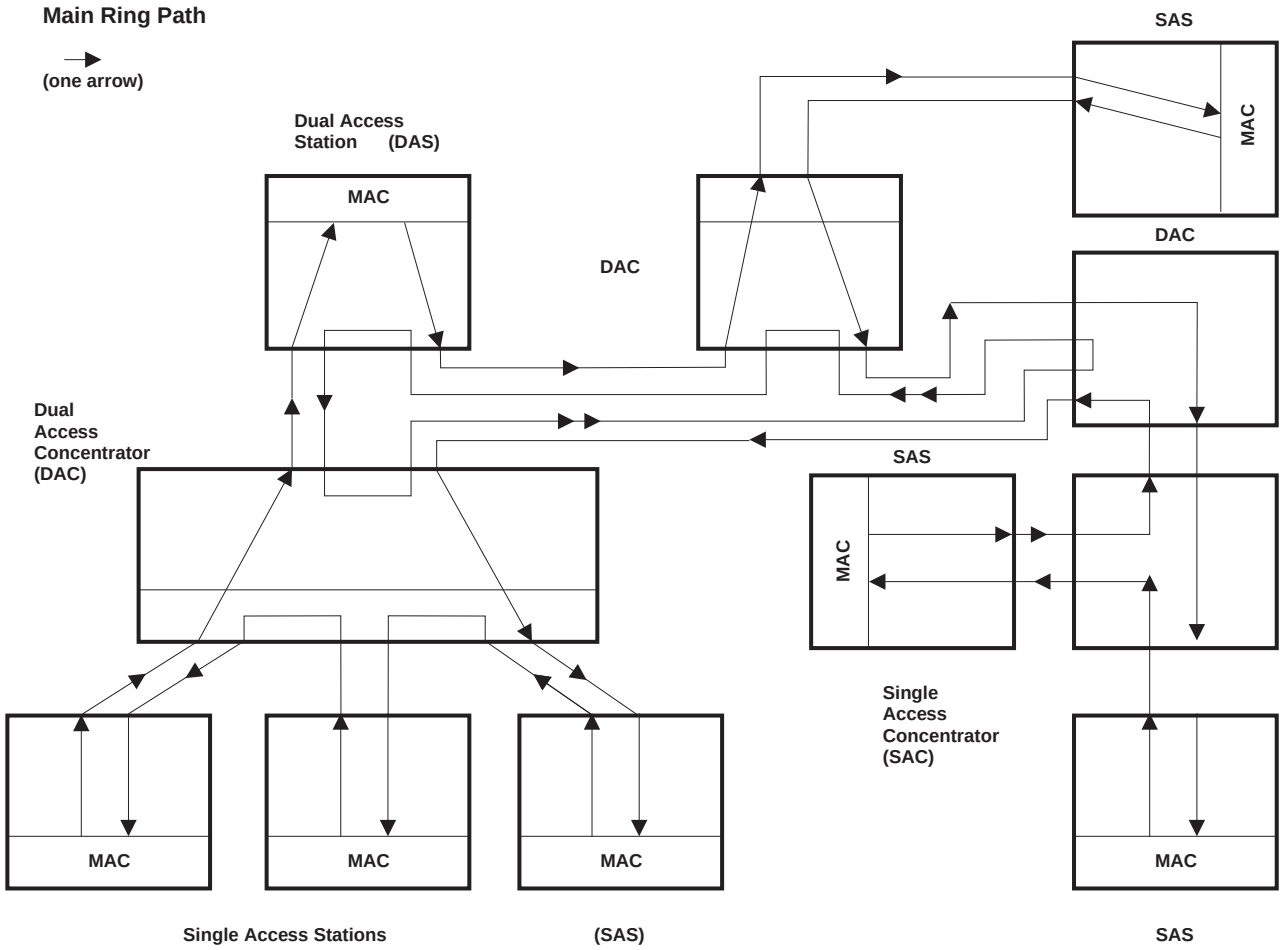


Figure 35. FDDI Network Diagram. This diagram shows Single Access Stations (SAS), Dual Access Stations (DAS), Single Access Concentrators (SAC), and Dual Access Concentrators (DAC) in one Main Ring Path of an FDDI network.

Chapter 17. Configuring and Monitoring FDDI

This chapter describe the FDDI interface configuration and operational commands. It includes the following sections:

- "Accessing the FDDI Configuration Commands"
- "FDDI Configuration Commands"
- "Accessing FDDI Monitoring Commands" on page 225
- "FDDI Monitoring Commands" on page 226

Accessing the FDDI Configuration Commands

You can access FDDI configuration from Talk 6. To do so, enter the **add device** command to add an FDDI interface to the network and assign an interface number to it, and then use the **network** command to access the FDDI interface as shown in the following example:

```
800 Config>  add device fddi
SK-NET FDDI device in slot 0 port 1 as interface #2
Use "net 2" to configure SK-NET FDDI parameters

800 Config>  network ?
0  :CHARM ATM Adapter
1  :ATM Token Ring LAN Emulation: elan1
2  :SK-NET FDDI

800 Config>  network 2
FDDI Interface Configuration
FDDI Config>
```

This will get you to the `FDDI Config>` prompt.

When you are finished, enter **Exit** to return to the previous prompt level.

FDDI Configuration Commands

This section describes the FDDI configuration commands as shown in Table 21. Enter the commands from the `FDDI Config>` prompt.

Table 21. FDDI Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
LLC	Provides access to the LLC configuration environment.
List	Displays the selected FDDI configuration.
Set	Sets FDDI parameters.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

List

Use the **list** command to display the current configuration for the FDDI.

Syntax:

list all

© Copyright IBM Corp. 1996, 1998

ler
pmf
tmax
tmin
treq
tvx
userdata

all Lists all of the output for the various parameters that follow.

ler Lists the link error rate alarms and cutoff values for port A and port B.
a -- lists the link error rate alarms and cutoff values for port A.
b -- lists the link error rate alarms and cutoff values for port B.

pmf Displays the PMF Password (maximum of 8 characters).

tmax Lists the Maximum Token Rotation Time (in milliseconds).

tmin Lists the Minimum Token Rotation Time (in milliseconds).

treq Lists the Requested Target Token Rotation Time (in milliseconds).

tvx Lists the Valid transmission timer expiration (in microseconds)

userdata
Displays the user data (maximum of 32 characters).

Set

Use the **set** command to configure FDDI.

Syntax:

set
ler
pmf
tmax
tmin
treq
tvx
userdata

ler port# type Sets the alarm and cutoff values for port A and port B as follows:

ler a alarm
Sets the alarm values for port A.

ler a cutoff
Sets the cutoff values for port A.

ler b alarm
Sets the alarm values for port B.

ler b cutoff
Sets the cutoff values for port B.

Valid values and defaults

Alarm or Cutoff	Valid Values	Default
Alarm	4 to 15	8
Cutoff	4 to 15	7

pmf Sets the PMF Password (maximum of 8 characters).

tmax Sets the Maximum Token Rotation Time (in milliseconds) that this station can accept. Commonly referred to in FDDI specifications as T_Max.

Valid values: 5 to 165 milliseconds

Default: 165 milliseconds

tmin Sets the Minimum Token Rotation Time (in milliseconds) that this station can accept. If the negotiated TTRT is less than this value, then the adapter will not provide proper service to the layers above it. Commonly referred to in FDDI specifications as T_Min.

Valid values: 5 to 165 milliseconds

Default: 5 milliseconds

treq Sets the Requested Target Token Rotation Time (in milliseconds) that this station will bid during initialization. Commonly referred to in FDDI specifications as T_Req.

Valid values: 5 to 165 milliseconds

Default: 165 milliseconds

tvx Sets the Valid transmission timer expiration (in microseconds). This timer is reset every time a valid frame or nonrestricted token is seen by the station. If the timer expires, it indicates that traffic is not circulating properly on the ring and therefore the claim process is started. Commonly referred to in FDDI specifications as TVX.

Valid values: 2500 to 10 000 microseconds

Default: 2500 microseconds.

userdata Sets the User data (maximum of 32 characters).

Accessing FDDI Monitoring Commands

You can access FDDI configuration from Talk 5 by entering the **network** command to access the FDDI interface as shown in the following example:

```
800+  network ?
0  :CHARM ATM Adapter
1  :ATM Token Ring LAN Emulation: elan1
2  :SK-NET FDDI

800 +  network 2
FDDI Interface
FDDI>
```

This will get you to the FDDI> prompt.

When you are finished, enter **Exit** to return to the previous prompt level.

FDDI Monitoring Commands

The monitoring commands for FDDI are:

Table 22. FDDI Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
List	Displays the FDDI adapter information
LLC	Displays the LLC monitoring prompt.
Srt-stats	Displays the FDDI bridging statistics.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to display the current FDDI configuration parameters.

Syntax:

list

Example:

```
 FDDI> list
MAC Address: 00:00:5A:00:00:01
```

Srt-stats

Use the **srt-stats** command to display the hardware assisted bridged statistics on this interface.

Syntax:

srt-stats

Example:

```
srt-stats
Port Supports:               Transparent Bridging Only

Frames received:                             806
Bytes received:                            34588
Maximum size of filter table in adapter:    4088
Number of entries in filter table:             0
Number of dynamic entries in filter table:     0
```

FDDI Interfaces and the GWCON Command

While the FDDI interfaces have their own monitoring processes for monitoring, the router also displays complete statistics for installed network interfaces when you use the interface command from the GWCON environment.

Statistics Displayed from FDDI Interfaces

The following statistics are displayed when you enter the **interface** *net#* command for a FDDI interface from the GWCON environment.

```
                                                Self-Test   Self-Test  Maintenance
Nt Nt'  Interface  Slot-Port                       Passed     Failed     Failed
0   0    FDDI/0    Slot: 1   Port: 1                 1          0          0

  IEEE 802.2/FDDI MAC/data-link on SK-NET FDDI interface
Address: 00:60:94:C4:00:40
UNA:     00:00:5A:02:2D:1E -> DNA: 00:00:5A:02:2D:1E
------------------------------------------------------------------------------
ECM State Machine:        IN
PCM State Machine Port A: SIGNAL
PCM State Machine Port B: ACTIVE
CFM State Machine Port A: ISOLATED
CFM State Machine Port B: CONCATENATED
CF State Machine:         C_WRAP_B
MAC Current Path:         PRIMARY
RMT State Machine:        RING_OP
------------------------------------------------------------------------------
TVX expired ct: 0
Beacon ct:      0
Claim ct:       0
RingOp ct:      1
------------------------------------------------------------------------------
PHYA:LEM_Ct:    0  LEM_Reject_Ct:    0  LCT fails: 40
     Alarm: 10°-8   Cutoff: 10°-7   Estimate: 10°-15
PHYB:LEM_Ct:    0  LEM_Reject_Ct:    0  LCT fails: 40
     Alarm: 10°-8   Cutoff: 10°-7   Estimate: 10°-15
------------------------------------------------------------------------------
T_Notify 10 sec, SMT frames in:55363  SMT frames out:35317
------------------------------------------------------------------------------
Frames:211764, Errors:0, Losts:0, Xmts:144058, Copied:171046, Not Copied:0
```

The following section describes general interface statistics:

Nt Global interface number

Nt' Applies only to dial circuits

interface
Interface name and number of this interface within interfaces of type ″intrfc″.

Port Port number

Slot Slot number

Self-Test Passed
Number of times self-test succeeded.

Self-Test Failed
Number of times self-test failed.

Maintenance Failed
Number of maintenance failures.

The following section describes the statistics displayed that are specific to the FDDI interfaces:

Address
Specifies the physical address of the FDDI interface.

UNA Specifies the physical address of the upstream neighbor.

DNA Specifies the physical address of the downstream neighbor.

ECM State Machine

Entity Coordination Management controls the management of the media interface, including all the ports at the node. It also controls the optical bypass.

```
OUT
IN
TRACE
LEAVE
PATH-TEST
INSERT
CHECK
DEINSERT
```

PCM State Machine

Physical Connection Management controls the management of the physical connection between a port being managed and another port in the adjacent node.

```
OFF
BREAK
TRACE
CONNECT
NEXT
SIGNAL
JOIN
VERIFY
ACTIVE
MAINT
```

CFM State Machine

Configuration Management manages the configuration of MACs and ports within a node.

```
ISOLATED
LOCAL
SECONDARY
PRIMARY
CONCATENATED
THRU
```

CF State Machine

Attachment configuration.

```
ISOLATED
LOCAL_A
LOCAL_B
LOCAL_AB
LOCAL_S
WRAP_A
WRAP_B
WRAP_AB
WRAP_S
C_WRAP_A
C_WRAP_B
C_WRAP_S
THRU
```

MAC Current Path

Current path which this MAC is inserted.

```
ISOLATED
LOCAL
SECONDARY
PRIMARY
```

RMT State Machine.

Ring Management controls the timing of the MAC management frames.

```
ISOLATED
NON_OP
RING_OP
DETECT_BEACON
NON_OP_DUP
RING_OP_DUP
DIRECTED
RM-TRACE
DETECT_CLAIM
DETECT_IDLE
```

TVX expired ct
Number of times TVX expired.

Beacon ct
Number of times beacon state entered.

Claim ct
Number of times claim state entered.

RingOp ct
Number of times ring has entered operational state.

LEM_Ct
Link error monitor error count.

LCT fails
Count of consecutive times the link confidence test has failed.

Alarm Estimate at which a link connection will generate an alarm.

Cutoff Estimate at which a link connection will be broken.

Estimate
Long term average link error rate.

Frames
Number of frames received.

Errors Number of frames detected in error.

Losts Number of format errors during reception.

Xmts Number of frames transmitted.

Copied
Number of frames copied.

Not Copied
Number of frames not copied.

T_Notify
Neighbor notification timer.

SMT frames in
Number of SMT frames received.

SMT frames out.
Number of SMT frames sent.

Monitoring FDDI

Part 2. ATM and LAN Emulation

© Copyright IBM Corp. 1996, 1998

Chapter 18. Overview of LAN Emulation

Note: See the glossary for definitions of the acronyms and terms used in this chapter.

The IBM 8210 implements the *LAN Emulation Over ATM: Version 1.0 Specification* which is widely accepted as the industry standard for multivendor multiprotocol interoperability. This chapter introduces basic LAN emulation (LE) concepts in the context of the MSS implementation. It begins by examining the motivation for installing emulated LANs (ELANs).

LAN Emulation Benefits

LAN emulation protocols allow ATM networks to provide the appearance of Ethernet and Token-Ring LANs. Although LAN emulation does not exploit all of the benefits of ATM, it is useful in migrating to ATM technology and lowering network management costs. It enables you to utilize high-speed ATM links and still protect your software and hardware investments.

Software investments are protected because application interfaces are unchanged (LAN emulation is implemented within the data link control layer, which is below the device driver interface of end stations). Hardware investments are protected with forwarding engines that bridge LAN and ATM networks so that existing adapters and wiring can continue to be used.

LAN emulation allows incremental installation of ATM adapters in stations with high-bandwidth requirements, for example, servers and engineering or multimedia workstations. Physical and logical views of a simple LAN emulation example are illustrated in 36.

© Copyright IBM Corp. 1996, 1998

Simple LAN Emulation Network

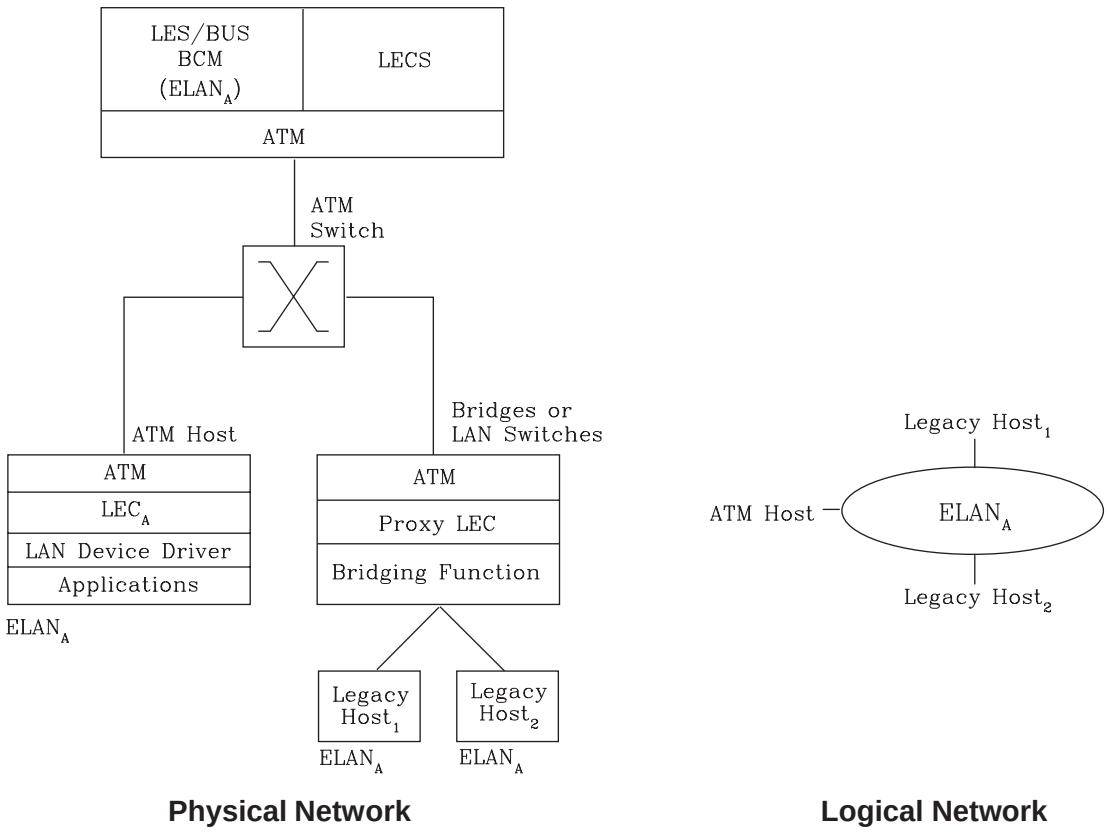


Figure 36. Physical and Logical Views of a Simple LAN Emulation Network

The network management benefits of emulated LANs (ELANs) come from increased flexibility in handling moves, adds, and changes. Membership in an ELAN is not based on physical location; instead, logically-related stations are grouped to form an ELAN (stations can also be members of multiple ELANs).

As long as ELAN memberships are retained, no reconfiguration is needed when stations move to new physical locations. Similarly, no wiring modifications are needed to move stations from one ELAN to another.

LAN Emulation Components

The following components implement an ELAN:

LAN emulation (LE) clients (LECs)
LAN emulation components that represent users of the Emulated LAN.

LE configuration server (LECS)
A LAN emulation service component that centralizes and disseminates configuration data.

LE server (LES)
A LAN emulation service component that resolves LAN destinations to ATM addresses.

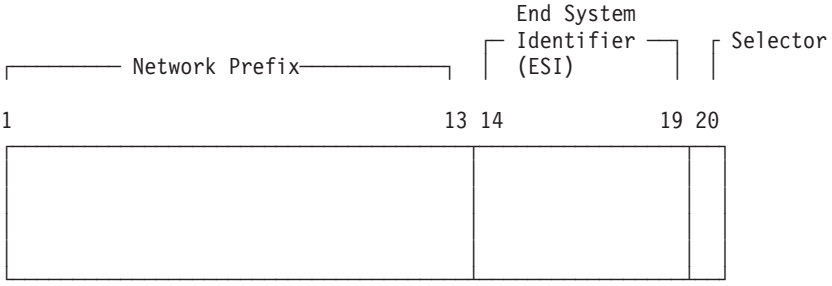
Broadcast and Unknown Server (BUS)
A LAN emulation service component responsible for the delivery of multicast and unknown unicast frames.

The LES, BUS, and LECS are collectively referred to as the LE service components. Each ELAN has a dedicated LES and BUS. LE clients reside in end systems, either in ATM-attached hosts or in bridges or LAN switches. The bridges or LAN switches represent hosts that are connected to Ethernet or Token-Ring LANs. LE clients provide a MAC-level service to higher level software. Either Ethernet IEEE 802.3 or IEEE 802.5 Token-Ring LANs can be emulated, but all stations on an ELAN must be of the same type.

The function that bridges between Token-Ring or Ethernet LAN segments and ELANs is called a Proxy LEC. To emulate a LAN, LE clients request services from the LECS, LES, and BUS. The following sections briefly review ATM addressing and pertinent Interim Local Management Interface (ILMI) functions. You need to understand these concepts before you can understand how the LE components function in the network.

Addressing in ATM

ATM uses 20-byte hierarchical addressing:



The first 13 octets of an ATM address are the Network Prefix. Each switch in your ATM network must have a unique Network Prefix. ATM switches use the Network Prefix to route VCC setup requests the destination ATM switch. End systems, like this router, retrieve their Network Prefix from their ATM switch when they activate.

Octets 14–19 of an ATM address are the End System Identifier (ESI). Each end system attached to the same switch must use a disjoint set of ESIs. When an end system activates, it attempts to register its ESIs with its ATM switch using the Interim Local Management Interface (ILMI).

The ILMI defines a set of SNMP-based procedures used to manage the interface between an end system and an ATM switch. End systems use ILMI to:

- Obtain the network prefix from the switch
- Register their ESIs with the switch
- Dynamically determine the UNI version of the ATM switch
- LECs may get a list of LECS addresses from the switch

The switch forces all of its registered ESIs to be unique.

Octet 20 of an ATM address is the selector.

End stations obtain their Network Prefix from the switch and form their own addresses by appending an ESI and selector. These addresses must then be registered with the switch, which rejects the registration if the ATM address is not unique.

ESI

Each ATM interface on the router has a universally administered, or burned-in, MAC address. You can use the MAC address as an ESI for some or all of the router's ATM addresses. Alternatively, you can define up to 64 locally administered ESIs on each interface. If every end system uses its universally administered MAC address as its ESI, then ATM addresses are guaranteed to be unique. This eases the configuration burden. However, using locally administered ESIs can ease problem determination. You can use any combination of universal or locally administered ESIs.

One way to obtain a unique ATM address is to use a burned-in IEEE MAC address as the ESI and to locally choose a unique selector. By default, the router uses the MAC address of the ATM interface as the ESI in its ATM addresses. Additional ESIs can be configured on each ATM interface.

Each ESI can have up to 255 associated selectors (0x00 through 0xff). The range of selectors is partitioned into two subranges, a configured selector range and an automatically assigned selector range. The ATM interface parameter max-configured-selector gives the upper bound on the configured selector range.

The ATM components on the router have various ways of choosing a selector. Some components require you to explicitly configure a selector from the configured selector range. LES/BUSs are an example of such a component. Other components, such as Classical IP clients, allow the selector to be automatically assigned at run-time. You do not have to choose the selector because the router does this when it activates. This selector is not guaranteed to be consistent across router restarts. Automatic selector assignment is useful only for those ATM components whose ATM address does not have to be already known by other network devices.

You must configure ATM before you configure emulated LANs, bridging or routing.

ATM Addresses of LAN Emulation Components

In general, ATM addresses must be unique among LAN emulation components. The only exception is that a LES and BUS serving the same ELAN can share an ATM address, as is the case on the server.

LAN emulation components are configured for a particular ATM interface. You can decide to use the burned-in MAC address as the ESI portion of the ATM address of the component or you can select one of the locally-administered ESIs that have been defined for the ATM interface. Multiple LE components can share the same ESI if they have unique selectors. By default, the configuration interface assigns each LE component a unique selector value for the configured ESI; however, you can override this assignment and explicitly configure a particular selector value.

An ATM interface parameter determines the number of selectors per ESI reserved for explicit assignment. The remainder are available for dynamic assignment by the ATM interface at run-time. LE components use only the selectors reserved for

explicit assignment; by default, 200 of the 256 possible selectors per ESI are reserved for explicit assignment. Run-time selector assignment is beneficial when you do not need to control the assigned selector, for example, when you are configuring clients in Classical IP that are not paired with an ARP server.

While ATM addresses must be unique among LE components, LE components can use the same ATM addresses as non-LE components, such as Classical IP servers.

Overview of Related ILMI Functions

ILMI defines a set of SNMP-based procedures used to manage the user-network interface (UNI) between an ATM end system and an ATM switch. The following three ILMI functions are particularly relevant to LAN emulation:

1. ATM address registration, which is described in “Addressing in ATM” on page 235
2. Dynamic determination of the signaling version being run at the switch
3. Acquisition of the LECS ATM addresses

As mentioned in “Addressing in ATM” on page 235, ATM address registration is a joint effort between ATM end systems and switches. ATM addresses must be registered with the switch before calls can be placed or received.

By default, the ATM interfaces of a server use ILMI procedures to query the switch MIB in an attempt to determine the signaling version (UNI 3.0 or 3.1) being run at the switch. If the query succeeds, the ATM interface runs the same UNI version as the switch; if the query fails, the ATM interface runs UNI 3.0. Alternatively, you can override the default and explicitly configure the UNI version that will run on the ATM interface.

Manual Configuration of the Signaling Version

You need to configure the signaling version manually if the ATM switch runs UNI 3.1 and has no UNI Version MIB variable. In this case, the ATM interface cannot dynamically determine the UNI version. Because the ATM interface in the server uses UNI 3.0 by default, you should manually configure the ATM interface to use UNI 3.1.

Locating the LECS Using ILMI

ILMI is the method of choice for locating the LECS. The ILMI MIB at the ATM switch includes a list of LECS ATM addresses that can be retrieved by LE clients. This method is useful because the LECS ATM addresses need only be configured at ATM switches, not at LE clients, and there are fewer switches than LE clients. Clients attempt to connect to the first LECS on this list. If the connection fails, they try the next LECS address in succession until a connection is established.

Overview of the LECS Function

LE clients are not required to use the LECS, although it is recommended. If the LECS is not used, each LE client must be configured with the ATM address of the LES that serves its ELAN. The LECS reduces the network management burden by serving as a centralized repository for configuration data, minimizing configuration of the LE clients.

Note: At most, one LECS is configurable on each server.

Clients connect to the LECS using well-defined procedures. The following steps are attempted by a client, in order, until a virtual channel connection (VCC) to the LECS is established:

1. Connect to the LECS using any configured LECS address information (configuration of an LECS ATM address at LE clients is optional and is ***not*** recommended).
2. Obtain a list of LECS addresses using ILMI and attempt to connect to each LECS on the list, in order, until a VCC is established.
3. Establish a VCC to the well-known LECS ATM address as defined by the ATM Forum.

As previously stated, ILMI is the preferred method for LE clients to locate the LECS. The well-known LECS address is needed because some switches do not support the ILMI method. Configuring the LECS address at the LE clients should be done ***only*** when the switch does not support the ILMI method and the LE service does not support the well-known LECS address.

The server and the IBM ATM switch support all three methods: the pre-configured LECS address, ILMI connection, and the well-known LECS ATM address.

The LECS must provide initial configuration data to LE clients. The most crucial piece of data is the ATM address of the LES. To provide this information to an LE client, the LECS must be able to identify the LE client and to determine the correct LES for that LE client. The LECS identifies an LE client using information in the LE_CONFIGURATION_REQUEST frame sent by the LE client. The configuration request can also contain information to identify the ELAN that the LE client is seeking to join. The following information can be included in the configuration request:

1. Primary ATM address of the LE client

   This field is required and uniquely identifies the LE client.
2. LAN destination associated with the LE client

   This field can contain a MAC address or a route descriptor that uniquely identifies the LE client or it can be unspecified.
3. ELAN Name

   This field can contain a name identifying the requested ELAN or the requesting LE client. In the server implementation, ELAN names are standard ASCII strings. The ELAN name can be unspecified in the request.
4. ELAN Type

   This field can specify that the LE client belongs to an Ethernet or Token-Ring ELAN, or it can be unspecified. If the LE client specifies the type of ELAN, the LECS cannot assign the client to an ELAN of a different type.
5. Maximum frame size supported by the LE client

This field can specify the upper bound on the size of a data frame that can be processed by the LE client, or it can be unspecified. The LECS cannot assign a client to an ELAN with a maximum frame size ***larger*** than that specified by the client. If the ELAN allows frames too large for the client to handle, the client cannot function on that ELAN.

Given this information, the LECS assigns the LE client to a LES. This is accomplished through the use of policies and policy values. A policy is a criterion that the LECS uses to make LE client-to-LES assignment decisions. A policy value is a (value, LES) pair that indicates that the specified value should be assigned to the specified LES. For example, a policy could be the MAC address of the LE client, and a policy value could be (MAC ADDR_A, LES_1). An LE client with MAC ADDR_A will be assigned to LES_1 if the LE client has not already been assigned to another LES because of a higher-priority policy. One set of policies and policy values applies to all the ELANs.

In accordance with the LE service MIB Specification of the ATM forum, these are the six policies defined:

1. ATM address
2. MAC address
3. Route descriptor
4. ELAN type
5. Max frame size
6. ELAN name

Policies also have priorities. The LECS examines policies in prioritized order. Policies with smaller values in the priority field are considered before policies with larger values in the priority field. Policies with equal values in the priority field are considered at the same time and *ANDed* together.

The LECS assigns an LE client to a LES when all of the policies at the current priority level are satisfied and in agreement. The policies are satisfied when there is a policy value that matches the corresponding field in the configuration request for each policy at the current level. The policies are in agreement when the set of matches include a LES that is common to all the policies. If these conditions are not met, the LECS considers the policies at the next priority level. If the LECS is unable to find a LES at any priority level, an unsuccessful configuration response is returned to the LE client.

To understand the meaning of agreement of the policies, consider this example of policies not in agreement. Suppose that the policies at priority 1 are a MAC address and an ELAN name. One of the policy values is (X'400000121225', LES_A) and one is (ELAN 1, LES_B). If the LE client provides a LAN destination of X'400000121225', the MAC address policy is satisfied. If the LE client provides an ELAN name of *ELAN 1*, then the ELAN name policy is also satisfied. In this case the policies at priority 1 are ***not*** in agreement because they refer to different LESs. In this example, the LECS would examine the policies at the next priority level.

After determining the correct LES for an LE client, the LECS returns a configuration response to the LE client that includes the following information: LES ATM address, ELAN type, max frame size, and ELAN name. The configuration response can also include type/length/value (TLV) parameters. TLVs provide a method to download optional or user-defined parameters to the LE client.

Sample Situations for Use of the LECS Assignment Policies

The following section offers examples of various LECS assignment policies.

ATM Address Policy

The LECS permits two types of ATM address policy values. The first type is a variable length ATM address prefix. For example, the policy value (399999999999900000102, LES_A) means that all LE clients whose ATM address begins with 399999999999900000102 should be assigned to LES_A.

The second type of ATM address policy value is an ESI and Selector of an ATM address. For example, the policy value (10002345003281, LES_A) means that the LE client with an ESI of 100023450032 and a selector of 81 should be assigned to LES A.

When given the ATM address of an LE client, the LECS searches first for a matching ESI and selector. If no match is returned, the LECS searches for the ATM address prefix policy value with the longest matching prefix. Thus, for example, the above policy value (399999999999990000, LES_B).

ATM address ESI and selector policy values can be used to assign clients to LESs in a manner independent of the LE clients physical location (the ESI and selector is defined locally to the client). ATM address prefixes are the only policy values which indicate any geographic information.

LAN Destination Policy

LE clients can be assigned to LESs based upon a MAC address or a route descriptor. Because a LAN destination uniquely identifies an LE client in a manner that is independent of geographic location, this policy is useful in ensuring that the LE client is assigned to the correct ELAN regardless of its physical location, for example, retaining the ELAN memberships of a workstation when it is moved from one switch to another.

ELAN Name Policy

ELAN names are perhaps the most flexible of the assignment criteria. Some of the ways that ELAN name policy values can be used are:

- Use the actual name of the ELAN

  If LES_A serves Elan 1, then create the policy value (Elan 1, LES_A). LE clients specifying Elan 1 in configuration requests will then be assigned to LES_A.
- Use aliases for the ELAN

  For example, all LE clients belonging to members of the Accounting Department could be configured to use the ELAN name *Accounting*, while those belonging to the Engineering Department could use the ELAN name *Engineering*. Depending upon the number of LE clients on the ELANs, these names could be directed to the same ELAN by configuring these policy values:

  ```
  (Accounting,  LES_A)
  (Engineering, LES_A)
  ```

  or to different ELANs by configuring these policy values:

  ```
  (Accounting,  LES_A)
  (Engineering, LES_B)
  ```

This setup requires configuring the LE clients with the correct ELAN Name.

- Use names for the LE clients

  Each LE client can be given its own name. For example, you could create the policy values (Joe, LES_A) and (Mary, LES_A). Then, the LE clients configured with these names would be directed to the same LES. This method requires configuring the ELAN name at each LE client and at the LECS. However, it allows Joe and Mary to move the client to a new location. Even though moving causes the client to have a new ATM address or MAC address, as long as you configure the new LE client with the same ELAN name, you retain membership in the original ELAN. This technique also offers a moderate amount of security if the names of each LE client are considered to be passwords.

ELAN Type Policy

ELAN type policy values are most useful for providing default ELANs. For example, the following policy values would ensure that every LE client is assigned to one of the LESs:

```
(Token-ring ELAN Type,  LES_A)
(Ethernet ELAN Type,    LES_B)
(Unspecified ELAN Type, LES_C)
```

In general, policies used for providing default ELAN assignments should be given a low priority, so that the more specific policies are considered first.

Max Frame Size Policy

The max frame size policy can also be used to provide default ELAN assignments.

Duplicate Policy Values

Duplicates occur when the same policy value is associated with multiple LESs for a given policy. Duplicate policy values are allowed for the ELAN type and max frame size policies, but are not allowed for other policies. Duplicate values are useful only when combined with a different policy of the same priority.

For example, assume that there are three ELANs: an Ethernet ELAN with a max frame size of 4544 bytes, a Token-Ring ELAN with a max frame size of 4544 bytes, and another Token-Ring ELAN with a max frame size of 18190 bytes. LE clients could be assigned to the appropriate ELAN by setting the ELAN type and max frame size policies to the same priority level and defining the following policy values:

```
(Ethernet ELAN Type,     LES_1)     (Max Frame Size = 4544,   LES_1)
(Token-Ring ELAN Type,   LES_2)     (Max Frame Size = 4544,   LES_2)
(Token-Ring ELAN Type,   LES_2)     (Max Frame Size = 18190,  LES_2)
```

More Information About TLVs

TLVs are defined on an ELAN basis; therefore, the same set of TLVs is returned to all LE clients that are assigned to a particular ELAN. When a TLV is included in a configuration response, the LE client ***must*** use the value specified in the TLV as an operating parameter (if the LE client recognizes the ELAN type). A few examples of situations where TLVs might be beneficial are as follows:

- When ELANs are spread over large geographic locations, the default timeout values for LE clients may be insufficient. These timeouts can be controlled for all LE clients by specifying their value in a TLV at the LECS.

- By default, ELANs use best-effort connections to connect to the BUS. For ELANs where BUS traffic is heavy, better performance can be obtained by using reserved bandwidth connections to the BUS. The characteristics of the Multicast Send VCC between the LE client and the BUS can be controlled with TLVs.
- A TLV can be used to download the ELAN segment number to source route bridges.

In addition to fine-tuning the configuration, TLVs force all clients on the ELAN to operate with consistent parameters. The IBM 8210 supports all ATM Forum-defined TLVs along with arbitrary, user-defined TLVs.

Connecting to the LES

After obtaining the ATM address of the LES, the LE client initiates a Control Direct VCC to the LES. When this VCC has been established, the LE client sends an LE_JOIN_REQUEST to the LES. The LES responds by adding the LE client to the appropriate point-to-multipoint Control Distribute VCC and returning an LE_JOIN_RESPONSE. By default, the LES partitions proxy and non-proxy clients onto separate Control Distribute VCCs as illustrated in Figure 37; however, you can configure the LES to use a single Control Distribute VCC for all LE clients in order to reduce the number of point-to-multipoint VCCs that are required. Partitioning the VCCs is generally useful because it reduces the amount of nuisance traffic that is sent to non-proxy clients. No LE_ARP_REQUESTs are sent to non-proxy LE clients, as described in “Address Resolution” on page 243.

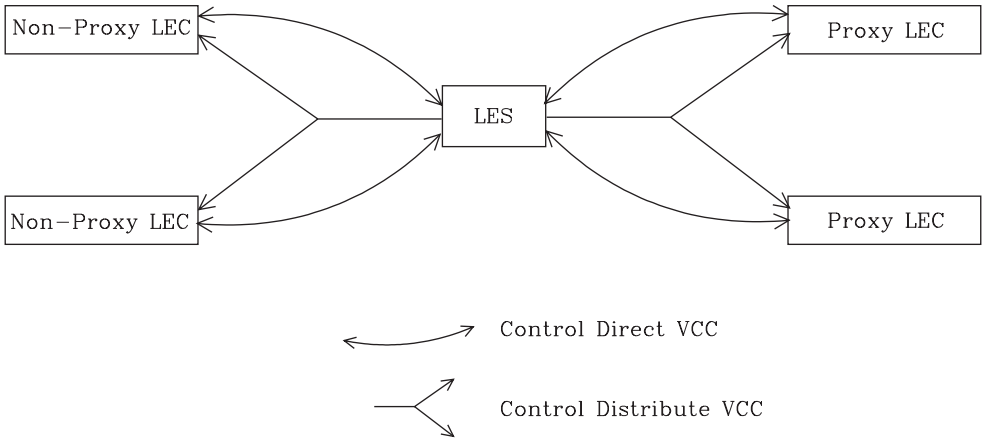


Figure 37. Default Connections Between LE Clients and the LES

The following ATM connections are established between the LE client and the LES:

Control Direct VCC (bidirectional point-to-point)
From LE client to LES

Control Distribute VCC (point-to-multipoint)
From LES to LE client

Address Registration

LE clients register LAN destinations with the LES to ensure uniqueness and to allow the LES to answer LE_ARP_REQUESTs, which LE clients issue to learn the ATM address associated with a particular LAN destination. Registrations include the LAN destination and the ATM address that the LE client associates with the LAN destination. A LAN destination can be either a MAC address or a route descriptor.

Proxy LE clients do not register the MAC addresses of stations on LAN segments that they are bridging to the ELAN. On the other hand, non-proxy LE clients must register all the LAN destinations that they represent. All route descriptors must be registered, regardless of whether they are associated with a proxy or a non-proxy LE client. Route descriptors are applicable only to proxy LECs that are performing source route bridging. A route descriptor contains the bridge number of the proxy LE client and the segment number of a ring that the LE client is bridging to that is equivalent to one hop away.

Address Resolution

LAN communications are based upon source and destination MAC addresses. To enable such communication on an ATM network, MAC addresses must be resolved to ATM addresses. An LE client sends an LE_ARP_REQUEST to the LES to learn the ATM address of a particular LAN destination. If the LAN destination is registered, the LES responds with the ATM address associated with the LAN destination. Otherwise, the request is forwarded to all proxy LE clients on the Control Distribute VCC. There is no need to forward the request to non-proxy LECs because all of their LAN destinations are registered; however, if the LES is configured to use a single Control Distribute VCC, both proxy and non-proxy LE clients will receive the request. Control Distribute VCCs provide an efficient way for the LES to distribute control frames to multiple LE clients.

Proxy LE clients respond to LE_ARP_REQUESTs for unregistered MAC addresses that they represent. The LE_ARP_RESPONSE is sent to the LES on the Control Direct VCC, and the LES forwards the response to the LE client that issued the request.

Connecting to the BUS

After connecting to the LES, an LE client issues an LE_ARP_REQUEST for the all 1s broadcast MAC address. The LES responds with the ATM address of the BUS. The LE client then initiates the establishment of a Multicast Send VCC to the BUS. The BUS responds by adding the LE client to the appropriate point-to-multipoint Multicast Forward VCC. By default, the BUS partitions proxy and non-proxy clients onto separate Multicast Forward VCCs; however, as was the case with the Control Distribute VCC, you can configure the BUS to use a single Multicast Forward VCC for all LE clients. Figure 38 on page 244 shows partitioned Multicast Forward VCCs.

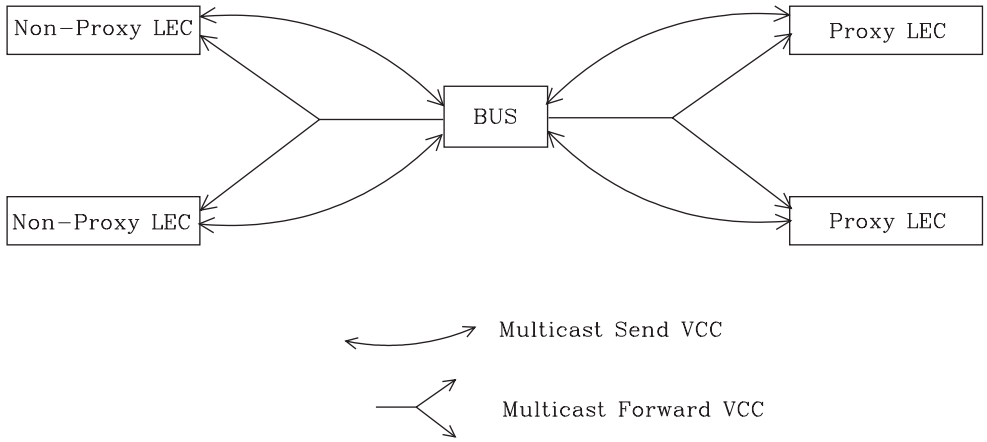


Figure 38. Default Connection Between LE Clients (LECs) and BUS

This list is provided to help you clarify the ATM connections that are established between the LE client and the BUS:

Multicast Send VCC (bidirectional point-to-point)
From LE client to BUS

Multicast Forward VCC (point-to-multipoint)
From BUS to LE client

BUS Functions

The BUS has two basic functions:

1. Distribute multicast frames to all the LE clients in the ELAN
2. Forward unicast frames to the appropriate destinations

An LE client sends unicast frames to the BUS if it does not have a direct connection to the LE client that represents the destination. To avoid creating a bottleneck at the BUS, the rate at which an LE client can send unicast frames to the BUS is limited.

In the server implementation, the BUS has two modes of operation: partitioning the unicast frame domain and not partitioning the unicast frame domain. If you partition the unicast frame domain, the BUS uses two Multicast Forward VCCs. Otherwise, the BUS uses a single Multicast Forward VCC.

If a single Multicast Forward VCC is used, the BUS operation is very simple; all received frames are simply forwarded to all LE clients. If two Multicast Forward VCCs are used, the BUS will not broadcast unicast frames to all LE clients; instead, unicast frames destined for non-proxy LE clients will be transmitted directly to the destination LE client on a Multicast Send VCC, and all other unicast frames will be transmitted only to proxy LE clients, using the Proxy Multicast Forward VCC. When two multicast VCCs are used, the server is considered to be in intelligent BUS (IBUS) mode.

IBUS mode reduces nuisance unicast frames, which are unicast frames not destined for the client; proxy clients do not receive unicast frames destined for non-proxy clients, and non-proxy clients never receive nuisance unicast frames. Network bandwidth devoted to nuisance frames is also reduced. On the other hand,

BUS processing requirements are increased and multicast frames must be transmitted twice (once on each Multicast Forward VCC). In general, IBUS operation is recommended; however, this option should be disabled in configurations that have source route bridges that join the ELAN as non-proxies.

BUS Data Packet Filtering

LAN Emulation depends on the emulation of traditional LANs using the LES-BUS to accomodate the shared media characteristics of Token Ring and Ethernet. The BUS provides the distribution function for all broadcast, multicast, and unknown unicast frames to other devices on the ELAN. Since all these frames must flow through the BUS, the BUS provides a natural location for controlling and managing ATM backbone data traffic.

You can use BUS Data Packet Filtering to allow specified types of data frames to be forwarded or discarded by the LANE BUS. Packets received by the BUS on a Multicast Send VCC can be verified against a list of enabled filters that you configure. Using this filtering mechanism, you have greater control over the type of traffic which is permitted on an ATM ELAN. The following types of filters are supported:

Protocol
: Allows data packets to be managed by protocol type: IP, IPX, Banyan Vines, NetBIOS, or AppleTalk, NetBIOS over IP, IP Multicast, IPX type 20, and BPDU.

MAC Address
: Manages packets by the MAC address in the Layer 2 packet header.

IP address
: Manages packets based on the IP address or subnet address.

Sliding window
: Manages data packets based on data in the packet located at a configurable packet offset. Offsets can be configured from the beginning of the MAC header or from the beginning of the information field. When using Token Ring, this information field is the byte following the RIF field. When using Ethernet, this information field is the information following the source address.

Data packet filtering occurs within an ELAN and is supported for both Ethernet and token-ring ELANs for all data frames received on a Multicast Send VCC. Each filter item is configured to provide a desired action: (exclude or include). Multiple filters of each action type may be configured. Each data packet is tested against each enabled filter in the configured filter list until a match occurs.

If you configure Exclude filters and Include filters, the **filter's preferred action** determines which filter list is first. If a match does not occur, the default action is performed on the frame.

Establishing Data Direct VCCs

Data Direct VCCs connect two LE clients, and are used to exchange unicast frames without involving the BUS. The LE client uses the address resolution procedures to determine the ATM address associated with the required LAN destination. If the LE client already has a Data Direct VCC to the ATM address (perhaps for another LAN destination represented by the target LE client), unicast data frames are

subsequently transmitted on the existing VCC; otherwise, the LE client invokes the signaling protocol to establish a new VCC.

The LE client maintains an LE_ARP cache containing LAN destination-to-ATM address mappings. Entries in this cache are aged and must be periodically refreshed. The entries are refreshed when a data frame is received from the LAN destination. The LE client also attempts to refresh entries in the absence of data traffic.

Utilization of Data Direct VCCs is also monitored and the VCCs are released if there is no traffic for the VCC time-out period, which is configurable. Additionally, Data Direct VCCs are released in a least-recently used manner when establishment of a new Data Direct VCC fails due to insufficient resource availability.

Overview of Extensions for LAN Emulation

IBM has made value-add extensions to ATM Forum LAN Emulation available on the server. These extensions offer improved performance, reliability, security, and manageability:

Broadcast Manager (BCM)
This function can improve overall network performance by reducing ELAN broadcasts.

Redundancy
The redundancy mechanism improves reliability by allowing backup servers to take over if failures occur at primary servers.

Security
Security is improved by letting the LECS control ELAN memberships.

BUS Monitor
This function enhances manageability by identifying the top users of the BUS.

The following sections describe each of these extensions.

Broadcast Manager

Broadcast Manager (BCM) is an extension to LAN emulation that consists of IBM enhancement of the LAN emulation BUS. Without BCM, the following events occur:

- A multicast frame sent to the BUS is forwarded to all LE clients on the ELAN.
- LE clients that include the proxy function to provide bridging support forward the broadcast frame on to other LAN segments.
- All end stations receive and process every broadcast frame.

BCM can be enabled on individual ELANs for any of these protocols:

IP

IPX

NetBIOS

When BCM is enabled, a minimal amount of layer 2 and layer 3 information is decoded for specific types of broadcast frames sent to the BUS. Whenever possible, BCM transforms broadcast frames into unicast frames, and sends them only to interested LE clients and end stations. BCM reduces both network traffic and

associated end-station overhead by filtering nuisance broadcast frames. These functions can improve overall system performance and enable practical deployment of larger ELANs.

BCM Support for IP

When enabled for IP, BCM scans all IP ARP requests and replies to learn the location of IP addresses in the IP subnet that contains this ELAN. The objective is for BCM to take each broadcast ARP request frame and forward it as a unicast frame directly to the LE client representing the target IP station. Both network traffic and end-station processing time are reduced when the request is forwarded directly to the appropriate LE client on the Multicast Send VCC instead of being broadcast to all LE clients on the Multicast Forward VCCs. When the destination station is located behind a bridge function, the LAN that the destination station belongs to also benefits from the reduced broadcast traffic.

BCM Support for IPX

For IPX, BCM limits the scope of advertisements and other broadcast requests. IPX routers and servers periodically broadcast their known network and service information. IPX clients send broadcast requests to locate a particular service or router. Generally, these broadcasts, called Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) packets, need to be received only by other IPX routers and servers.

When it is enabled for IPX, BCM dynamically identifies the set of IPX routers and servers based on advertisement transmissions, and only forwards RIP and SAP advertisements and other broadcast requests to other IPX routers and servers. A broadcast frame managed by BCM IPX is sent as a series of unicast frames to the dynamically-learned set of IPX routers and servers.

When BCM IPX Server Farm Detection is enabled, BCM IPX will detect an IPX server farm when the number of IPX routers and servers discovered behind a given LEC exceeds a configurable threshold, the *BCM IPX Server Farm Threshold*. When a server farm is detected, BCM IPX broadcasts a managed frame to each LEC representing a server farm, rather than transmitting multiple unicast frames to each downstream IPX router and server in the server farm. BCM IPX can now intelligently use the broadcast mechanism in areas of the network where it is desirable to do so.

With BCM IPX enabled, any quiet device (that is, a device that does not transmit IPX advertisements) that needs to receive IPX advertisements has to be configured as a BCM static target. An example of such a device is a station running software that discovers the IPX network topology by monitoring IPX advertisements.

If BCM IPX Server Farm detection is enabled and you wish to prevent a particular LEC from being treated by BCM IPX as a Server Farm, configure a BCM static target with the LEC's ATM address and a MAC address of 00.00.00.00.00.00. This forces BCM IPX to send frames managed by BCM as multiple unicast frames to each downstream IPX router and server detected behind this LEC, even if the number of routers and servers detected exceeds the *BCM IPX Server Farm Threshold*.

BCM Support for NetBIOS

NetBIOS is considered to be a broadcast-abusive protocol and therefore an excellent candidate for BCM. NetBIOS communication is based on names. Transmitting stations can learn the MAC address associated with a particular destination name by broadcasting a query or by having the frame multicasted to the NetBIOS functional address. In the latter case, every NetBIOS device in the network must receive the frame and determine whether the destination name on the frame applies to itself. To make things even worse, NetBIOS devices tend to repeat transmission of certain types of frames as much as 10 times. Historically, this was to ensure that all devices receive the frame in cases where the network is heavily congested.

The BCM strategy is to associate unique NetBIOS names with MAC addresses and LE clients by learning names from NetBIOS frames sent to the BUS. After a unique NetBIOS name is learned, subsequent NetBIOS broadcast frames destined for that name are forwarded to a single LE client as a unicast frame. BCM also filters certain NetBIOS frames that are broadcast repeatedly.

BCM provides support for NetBIOS Namesharing. That is, BCM NetBIOS handles OS/2 LANServer stations with multiple LAN adapters sharing the same NetBIOS name.

BCM Support for Source Route Bridging

Source Route Management (SRM) is an additional BCM feature that can be configured for 802.5 ELANs. When enabled, this feature will further process frames managed by BCM IP or BCM NetBIOS and, whenever possible, transform All Routes Explorer (ARE) or Spanning Tree Explorer (STE) frames into Specifically Routed Frames (SRF). Once a frame is transformed into an SRF, the frame no longer needs to be transmitted onto each ring in the bridged network.

The Token-Ring topology behind each LE client is learned by recording the routing information field (RIF) of frames received by the BUS. Because SRM dynamically learns Token-Ring topology information, an aging mechanism is used to remove information that has not been refreshed recently.

To decide whether to enable BCM or SRM (or both), you should compare the net system-wide benefit with the inevitable reduction in the rate at which packets are forwarded when BCM or SRM is enabled.

Note: Broadcast Manager and Source Route Management are unavailable and cannot be enabled if **bus-mode** is set to *adapter* or *vcc-splice*.

LAN Emulation Reliability

A perceived lack of robustness has been one of the most widely proclaimed criticisms of LAN emulation. While the ATM Forum is addressing this issue with specifications for distributing the LE service, the server offers an answer in the interim. Figure 39 on page 249 provides a framework for describing the MSS redundancy solution.

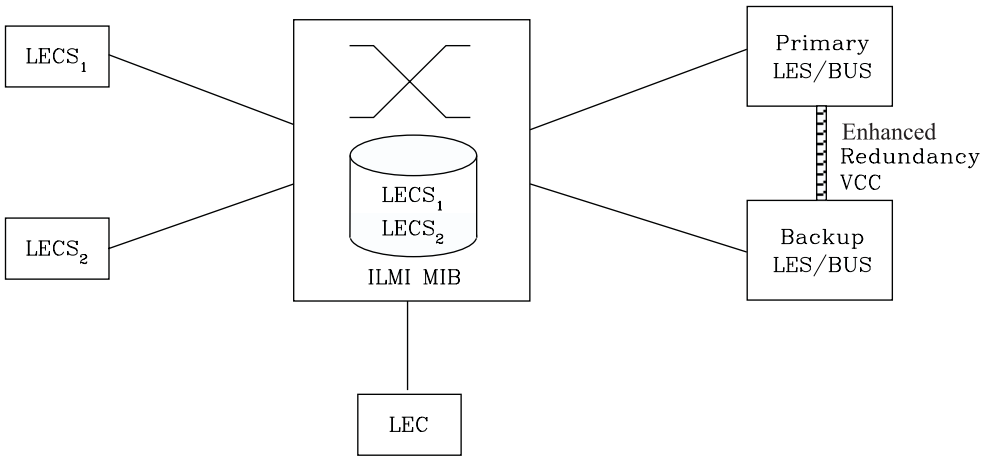


Figure 39. LAN Emulation Redundancy

Each LES/BUS may be independently configured for redundancy (the default is no redundancy). If redundancy is enabled, the LES/BUS is configured to assume the role of a primary or a backup LES/BUS. Unless it has been configured as a redundant LES/BUS, the LES/BUS is primary. The primary LES/BUS is typically the only LES/BUS visible to the LE clients. It is responsible for setting up and maintaining an Enhanced Redundancy VCC to the backup LES. The presence of this VCC and timely status messages indicate that the primary LES/BUS is operational.

If the Enhanced Redundancy VCC is ***not*** present, the backup LES/BUS services ELAN requests in the usual manner. If the backup LES/BUS is servicing the ELAN when the Enhanced Redundancy VCC is established by the primary, the behavior is determined by the setting of LES/BUS Peer Redundancy Support.

Enabling Peer Redundancy support allows clients to remain active on the backup LES/BUS even after the Enhanced Redundancy VCC is established between the primary and backup LES/BUS. When Redundancy support is enabled, but Peer Redundancy is disabled, the backup terminates all its clients when the Enhanced Redundancy VCC is established, always yielding to the primary LES/BUS. When Redundancy and Peer Redundancy support are both enabled and the Enhanced Redundancy VCC is up, the primary and backup LES/BUS periodically transmit status messages to one another containing the number of active clients. In the event that the primary and backup LES/BUS each has active clients at the time when the Enhanced Redundancy VCC is established, the LES/BUS with the lower number of active clients terminates its clients, yielding to the LES/BUS with the higher number of active clients. If the number of active clients is equal, the backup LES/BUS yields to the primary. In order to give preference to the primary LES/BUS in the race condition where primary and backup become operational at approximately the same time, the backup will yield to the primary if the Enhanced Redundancy VCC is established within one minute of the backup registering itself with the ATM switch.

For simplicity, only the Primary LES/BUS has the Peer Redundancy option. Peer Redundancy is disabled by default to maintain the redundancy behavior of prior releases of server software.

For the redundancy protocol to be effective, LE clients must detect the failure of the primary LES/BUS and connect to the backup. LE clients detect server failures by means of released VCCs. Connection to the backup LES/BUS is accomplished through the LECS.

Upon receiving an LE_CONFIGURE_REQUEST, the LECS assigns the LE client to the appropriate LES and ELAN. If this LES has no configured backup, then the LECS returns the ATM address of the LES. If the LES is configured with a backup LES, then the LECS returns either the primary or backup LES address.

The LECS returns the backup LES address if the backup LES exists on the same MSS Server as the LECS and is currently serving the ELAN, if the primary LES exists on the same MSS Server as the LECS and it is not currently serving the ELAN, or if neither LES exists on the same MSS Server as the LECS and the client was last assigned to the primary LES (within the past 5 minutes). Otherwise, it returns the primary LES address to the LE client.

The LECS retains a short-term memory of all client assignments so that it can alternately direct an LE client to a primary and backup LES. This simple heuristic makes the correct assignment in the nominal case of no failure and is self-correcting. At worst, the heuristic causes the LE client to repeat the configuration phase of joining an ELAN.

LECS robustness can be achieved by establishing duplicate LECSs on multiple platforms and including their ATM addresses in the ILMI database. LE clients will then connect to the backup LECS if the primary is unavailable. For example, LECS 1 and the backup LES/BUS in Figure 39 on page 249 could be on MSS Server 1, while LECS 2 and the primary LES/BUS could be on MSS Server 2.

Additionally, note that servers need not be dedicated to backup functions, because a single server can host backup LES/BUSs for some ELANs and primary LES/BUSs for other ELANs.

LAN Emulation Security

Traditional LANs offer security in the sense that a physical connection implies that two stations are on the same LAN. Because multiple emulated LANs can exist on a single ATM network, stations that are not on the ELAN can be physically connected to stations that are on the ELAN. This situation presents a security risk in that unauthorized stations can connect to the LES and attempt to use its services.

To control ELAN membership, an MSS LES can be configured to validate LE_JOIN_REQUESTs with the LECS. In this mode the LES forms an LE_CONFIGURE_REQUEST on behalf of the LE client using information from the LE_JOIN_REQUEST. These LE_CONFIGURE_REQUESTs include the source LAN destination, source ATM address, ELAN type, max frame size, and ELAN name from the LE_JOIN_REQUEST, along with an IBM Security TLV. The security requests are transmitted to the LECS by a multiplexing component called the LECS interface, and the LECS must validate the requests using its ELAN assignment database before LE clients are allowed to join the ELAN.

A LECS interface is associated with an ATM interface, and all LESs configured on the ATM interface use the same LECS interface. The LECS interface conserves VCC resources by multiplexing security requests from multiple LESs onto a single

VCC to the LECS. The LECS interface locates the LECS dynamically using the ILMI and well-known LECS address mechanisms. After the VCC to the LECS is established, the LECS interface issues a local query to determine whether the LECS is located on the same server. If the LECS is located on the same server, a local interface is used to confirm requests to join without transmitting requests onto the ATM network.

With the LECS interface, the server may ensure that an LE Client joins an ELAN only if the LECS approves of the join. This shifts the security burden from the LES to the LECS. Unfortunately, the LECS is also non-secure. The LECS accepts connections and queries from any station without verification. An intruder station may connect to the LECS and repeatedly query it for various configurations. The intruder may also pose as some other station and download another station's configuration.

LECS Access Controls permit the user to configure a list of ATM address prefixes which are not allowed access to the LECS configuration database. All LECS connection attempts and LE_CONFIGURE_REQUESTs from matching ATM addresses are automatically rejected. When used in conjunction with the LECS interface, a secure LANE environment is provided.

To maximize the security of an ELAN, the following steps are recommended:

1. At the LECS, use ATM addresses to assign clients to the LES. See "Overview of the LECS Function" on page 238 for more information.
2. Activate the LECS Interface on the server.
3. Activate the security option of the LESs.
4. Activate LECS Access Controls for any ATM address prefixes that should not be allowed to access the LECS.
5. Use *Address Screening* at the ATM switches. This option causes switches to validate that calling stations use their actual ATM addresses in the call setup. Thus, stations cannot impersonate other stations.

These steps ensure that stations are correctly identified and that only authorized stations join the ELAN.

BUS Monitor

The BUS Monitor provides a way to pinpoint end users who may be over-utilizing the BUS. When enabled, the BUS Monitor periodically samples the traffic sent to the BUS on a particular ELAN. At the end of each sample interval, the BUS Monitor identifies the top users of the BUS by their source MAC addresses, LE client ATM addresses, and the number of sampled frames each of them has sent to the BUS. You can configure the following parameters for the BUS monitor:

- The number of MAC addresses (hosts) to record as top users
- The number of seconds in each sample interval
- The sample rate. The sample rate consists of the fraction of all the frames received that the sample consists of, for example, 1 out of every 100 frames, 1 out of every 10 frames, or every frame.
- The number of seconds between sample intervals

BUS Police

The BUS Police function uses BUS Monitor to provide dynamic BUS traffic management. BUS traffic is managed by sampling BUS data traffic and dynamically installing BUS MAC filters for devices that exceed the value of bus usage threshold.

If you do not want traffic from a particular device, such as routers or SNMP network management stations, to be filtered from the BUS, you can add that device to the immunity list. Devices on the immunity list are exempted from BUS policing. These immune devices will continue to be monitored and information about the traffic they generate may be listed in BUS Monitor results if they are one of the top users of the BUS.

LECS Database Synchronization

You can configure ELANs on a single primary LECS and then invoke a single command to copy the LECS configuration to one or more IBM 8210 servers with designated redundant LECSs using LECS database synchronization. You can also have the LECS configuration automatically copied to the secondary LECSs whenever the primary LECS is restarted or the server reboots.

Use the **database-synchronization** command at the `LECS config>` command prompt to configure a list of remote secondary LECS addresses that will be synchronized with the primary LECS.

SuperELAN

SuperELAN is essentially the precursor to LAN Emulation Network to Network (LNNI) specification currently being addressed by the ATM Forum LAN Emulation standards committee. SuperELAN provides distributed LE services for version 1.0 emulated LANs.

A SuperELAN is a collection of emulated LANs. A client on any of the SuperELAN member emulated LANs can set up a data direct VCC to any other client on the SuperELAN. In essence, a SuperELAN emulates a standard ELAN, distributing the LE services among the member ELANs. The reliability and performance of the LE services increases with the number of ELANs. Resource utilization becomes less centralized, allowing a SuperELAN to be much larger than a standard ELAN.

Distributing LE services is accomplished by logically linking together individual ELANs. When ELANs are linked together in a SuperELAN, certain LAN Emulation control frames (such as LE ARP requests and LE ARP responses) and data frames are forwarded between the member ELANs. By forwarding certain LE control frames, clients are able to locate a target client on another ELAN and establish a data direct VCC to it.

Data Direct VCCs between ELANs also utilize the switched fabric of the ATM network. Although each LE server still exhibits a concentration of utilization, no single LE server serves the entire SuperELAN, and network utilization is distributed among the constituent LE servers. Thus, SuperELAN LE Services can serve larger numbers of clients.

Because a SuperELAN is made up of multiple ELANs, reliability is improved. If one LE server fails, other LE servers within the SuperELAN are not affected. Only the

inter-ELAN data-direct VCCs to clients in the failed ELAN are affected. In addition, clients that were joined to the failed ELAN can be configured to join one of the other SuperELAN LE services by requesting another LES address from the LECS.

The propagation of broadcast and unknown frames is a major concern within a SuperELAN network. Both types of frames are forwarded to every member ELAN except the ELAN from which the frames were received. This forwarding uses bandwidth on every segment of the network, and, in the case of broadcast frames, causes an interruption at every station.

A SuperELAN is equipped with two additional functions to combat the effects of these frames.

Bridging Broadcast Manager (BBCM) can transform many broadcast frames into unicast frames, thus lessening their effects on network performance. BBCM snoops on packets to learn bindings between layer 3 and layer 2 network addresses. Future broadcast packets to any learned layer 3 address can be transformed into unicast packets and forwarded by the bridge as any other unicast packet. If the transformed unicast address is in the bridge database, then the packet can be forwarded to its destination segment. The packet will not cause an interruption at every station, nor will it utilize bandwidth on every network segment.

Dynamic Protocol Filtering (DPF) also snoops on packets. It learns the different protocols being received on every bridge port. Packets for a particular protocol are not forwarded over ports that are not actively using that protocol. Although many bridges permit filtering based on protocol, DPF performs this filtering automatically based on current traffic.

Refer to the chapter entitled “Bridging Features” in the *Multiprotocol Switched Services (MSS) Configuring Protocols and Features* for more information about BBCM and DPF.

SuperELAN, aided by Bridging Broadcast Manager and dynamic protocol filtering, combine to provide a reliable, distributed, emulated LAN with strong controls on the propagation of broadcast and unknown frames.

SuperELAN II

SuperELAN II is the enhanced successor to SuperELAN. SuperELAN II supports the following additional new functions:

- Source-Route ATM Token Ring Topologies
- Multiple SuperELANs in a single device
- Independent operation from existing ASRT bridging function

SuperELAN II is based on a source-route aware transparent LAN Emulation bridge technology. LAN Emulation control frames are bridged as described in “SuperELAN” on page 252, and data frames are bridged using the new SuperELAN II bridge path while the data direct VCC is being established. All data frames forwarded between ELANs in the SuperELAN use the transparent MAC and/or Route Descriptor cache to forward non-broadcast unicast traffic. All broadcast frames are treated like Spanning Tree Explorer frames and are forwarded onto every ELAN in SuperELAN Spanning Tree forwarding state.

Each SuperELAN maintains independent MAC, LE Control Frame, BBCM, VLAN, and Route Descriptor (Token Ring only) forwarding caches. Multiple SuperELANs

can be bridged together using the ASRT bridging function (This is especially useful for interconnecting Ethernet and Token Ring SuperELANs using SR-TB).

Distributed SuperELANs can be constructed using multiple devices.

The existing SuperELAN support under the ASRT bridging function is still supported. Refer to the chapter entitled “Bridging Features” in the *Multiprotocol Switched Services (MSS) Configuring Protocols and Features* for more information.

BBCM, Dynamic Protocol Filtering VLANs, and MAC filters are all supported in SuperELAN II. Static bridging filters like SAP and or NetBIOS name filters, manual Spanning Tree port control, and IP Host bridge support are not currently supported.

SuperELAN users should review their current network configuration prior to migrating the MSS configuration to SuperELAN II to insure that SuperELAN II meets their network requirements. See “Migration to SuperELAN II” on page 260.

Key Configuration Parameters for LAN Emulation

This section briefly describes the required configuration parameters of the server LAN emulation components. The ATM interface for the LAN emulation components must be defined before the components can be created.

1. **LEC**:

   To create an LE client, you only need to specify the ELAN type. If you define two LE clients on a single ATM interface and bridge them together, then one of the LE clients must use a non-default MAC address. By default, LE clients use the burned-in MAC address of the ATM interface. The default maximum frame size is 1516 bytes for Ethernet LE clients and 4544 bytes for token-ring LE clients.

2. **LES/BUS**:

   The required parameters for a LES/BUS are the ELAN name, the ELAN type, and the ESI (which you select from a list that includes the burned-in MAC address and any locally-administered values defined for the ATM interface). Defaults are supplied for other parameters.

   The maximum frame size default is 1516 bytes for Ethernet ELANs and 4544 bytes for Token-Ring ELANs. LE clients will not be allowed to join the ELAN if their maximum frame size is less than the maximum frame size of the ELAN; LE clients that have a larger maximum frame size will be allowed to join the ELAN, but will use the maximum frame size of the ELAN as a result of join-time negotiation with the LES.

3. **LECS**:

   At a minimum, you must select the LECS ESI and configure a default ELAN assignment policy. See “Overview of the LECS Function” on page 238 for more information.

Chapter 19. Using ATM

This chapter describes how to use the ATM interface. It includes the following sections:

- "ATM and LAN Emulation"
- "How to Enter Addresses"
- "ATM-LLC Multiplexing" on page 256
- "ATM Virtual Interface Concepts" on page 265

ATM and LAN Emulation

LAN emulation provides support for virtual Token-Ring and Ethernet LANs over an ATM network. Refer to "How to Enter Addresses" for a discussion of ATM addressing.

How to Enter Addresses

Enter addresses in two ways, depending upon whether the address represents (1) an IP address, or (2) an ATM address, MAC address, or route descriptor, as follows:

1. IP address

   Enter IP addresses in dotted decimal format, a 4-byte field represented by four decimal numbers (0 to 255) separated by periods (.).

   Example of IP Address:

   ```
   01.255.01.00
   ```

2. ATM or MAC address or route descriptor

   Enter ATM addresses, MAC addresses, and route descriptors as strings of hexadecimal characters with or without optional separator characters between bytes. Valid separator characters are dashes (-), periods (.), or colons (:).

   Examples of ATM address, MAC address or route descriptor

   ```
   A1FF01020304
       or
   A1-FF-01-02-03-04
       or
   A1.FF.01.02.03.04
       or
   39.84.0F.00.00.00.00.00.00.00.00.00.03.10.00.5A.00.DE.AD.08
       or
   A1:FF:01:02:03:04
       or even
   A1-FF.01:0203:04
   ```

   Each type of address requires a different number of hexadecimal characters:

   ATM 40

   MAC 12

   ESI 12

   Route descriptor
   4

© Copyright IBM Corp. 1996, 1998

This information applies to addresses entered for ATM, LAN emulation, Classical IP and ARP over ATM, IPX over ATM, and ARP over ATM.

ATM-LLC Multiplexing

Protocols that run natively over an ATM interface can use ATM-LLC multiplexing to share ATM addresses and both SVC and PVC channels between users. ATM-LLC is implicitly configured when the protocols are configured and can be monitored using the `ATM Config+` command prompt from **t 5**. There are no explicit configuration options for the ATM-LLC multiplexing function. For example, if two protocols which use ATM-LLC multiplexing are configured to use the same local ATM address (local endpoint), this implicitly configures ATM-LLC to use the same shared ATM address for both protocols.

See “ATM-LLC Monitoring Commands” on page 281 for additional information.

Sharing of ATM addresses or SVC/PVC channels is not possible between protocols that use the ATM-LLC multiplexing function and those that do not use the ATM-LLC multiplexing function (such as Classical IP). Currently, Server Cache Synchronization Protocol (SCSP) and APPN are the only two protocols that use the ATM-LLC multiplexing function.

ATM SuperELAN II Configuration Concepts

The concept of SuperELANs is discussed in the chapter entitled “Bridging Features” in the *Multiprotocol Switched Services (MSS) Configuring Protocols and Features*. Reasons for using SuperELANs for building large ATM LAN Emulation networks can be grouped into two categories:

- Improved ATM LAN Emulation network performance
- Improved ATM LAN Emulation network reliability

Using a SuperELAN to combine multiple ELANs with fewer clients instead of placing all clients on one large ELAN can:

1. Improve VCC setup times since clients can be distributed across multiple LES/BUSes in different switches
2. Reduce the impact of failure of one LES/BUS on network connectivity, since clients in the other ELANs remain active
3. If bridging, improve the inter-ELAN data traffic transmission speed since inter-ELAN data traffic is transmitted at hardware switching speed along a direct path because the software necessary to perform bridging is no longer in the middle of the client-to-client communication.

With the appropriate network design utilizing multiple ATM switches, LES/BUSes, LECSs, and SuperELANs, a high performance redundant ATM LAN Emulation network can be configured to provide reliable high bandwidth communication.

Configuring a SuperELAN II

Once the LES/BUSes have been configured for each ELAN (LES/BUSes are not required to be located in the same device as the SuperELAN. See “Chapter 24. Using LAN Emulation Services” on page 349 for information about configuring LES/BUSes.),

1. Use the SE-SERVICES **add** command to add a SuperELAN.

2. Use the **work** command to select the SuperELAN just added.
3. Add each ELAN to the SuperELAN using the **add elan to superelan** command.

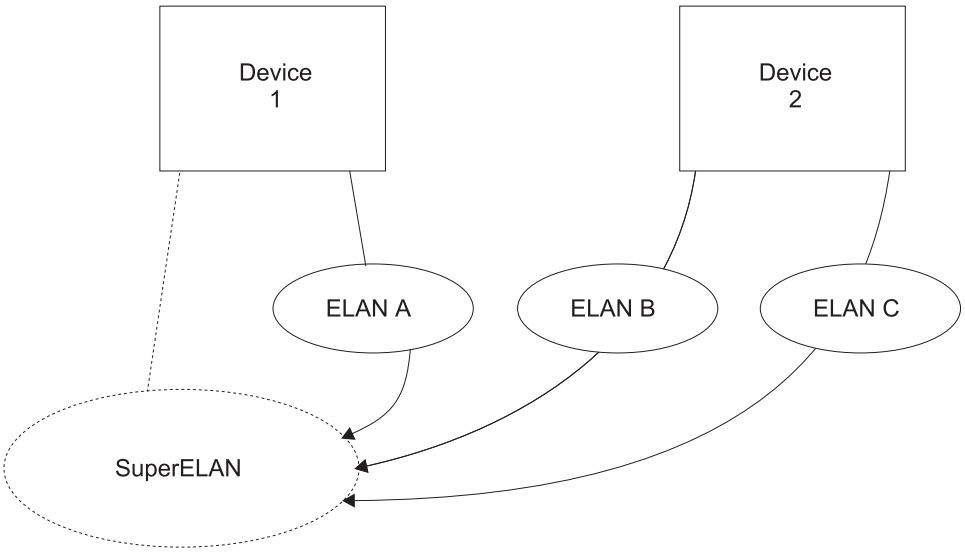


Figure 40. Adding ELANs to Form a SuperELAN

The **add elan to superelan** command will present a list of locally configured ELANs and an option to add an remotely configured ELAN. Only those ELANs allowed to participate in the SuperELAN will be displayed.

ELANs may not be displayed because:

a. ELAN type does not match the SuperELAN type, either Ethernet or token-ring
b. ELAN frame size does not match the SuperELAN frame size
c. ELAN is on an ATM interface with a different network ID than that of the SuperELAN
d. ELAN is currently configured in another SuperELAN

Remote ELAN configurations must conform to the above four conditions for proper SuperELAN operation.

4. Use the **broadcast-manager**, **set**, and **vlan** commands to tune the SuperELAN.

   Cache parameters, broadcast management, VLAN enablement, and MAC filters may be configured to enhance the performance of the SuperELAN. See the chapter entitled “Using and Configuring MAC Filtering” in *Configuring Protocols and Features* for information about configuring MAC filters.

SuperELAN II Spanning Tree

Each SuperELAN runs an independent, modified, 802.1d spanning tree. This insures that there are no SuperELAN loops in the network and that each ELAN receives at most one copy of a unknown unicast, broadcast frame, or LE Control frame. Bridges running a true 802.1d or the Token Ring bridging spanning tree do not participate in the SuperELAN spanning tree nor does the SuperELAN participate in bridging spanning trees. This means that from a bridging spanning tree perspective, the SuperELAN appears as a single network segment. As shown in Figure 41 on page 258, bridges connected to different ELANs in a SuperELAN and

also connected to the same legacy network, either directly or through another bridge, are considered to be in parallel.

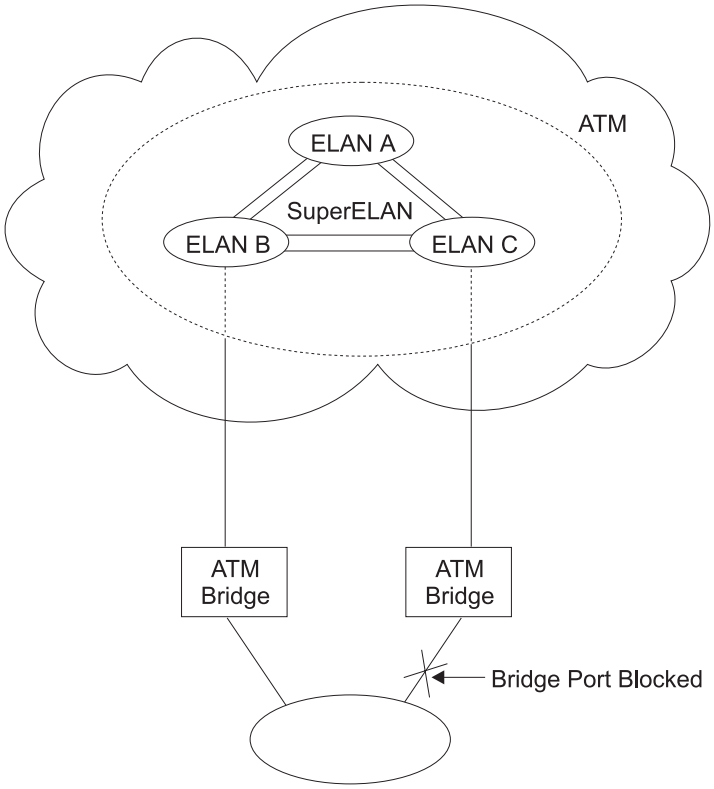


Figure 41. Parallel SuperELANs

Unlike the 802.1d Spanning Tree Protocol (STP) frames, the destination MAC address of the SuperELAN II STP frames is the all 1's broadcast address instead of the bridge functional address. Therefore, other non-SuperELAN bridges connected to the SuperELAN will forward these STP frames onto other LANs and ELANs. Although harmless, it may be useful to reduce this extraneous traffic by filtering these SuperELAN II STP frames in the other bridges. This can be accomplished by adding a SNAP filter for SNAP header `10005A-80D7` in the other bridges.

Redundant SuperELANs

Redundant SuperELANs provide inter-ELAN connectivity in the event one or more devices fail. Redundant SuperELANs can be constructed using multiple devices. In Figure 42 on page 259, a second SuperELAN is added to the second device with the same SuperELAN ID as the first device. Both SuperELANs (which may have different SuperELAN names) contain ELAN A, ELAN B, and ELAN C. One possible SuperELAN spanning tree scenario is shown in Figure 43 on page 259. If device 1 fails, the SuperELAN forwarding paths 2b and 2c will move to forwarding state from blocked state. Clients joined to ELAN A should return to the LECS and be assigned to either ELAN B or ELAN C. SuperELAN paths 1a, 1b, and 1c will cease to exist. Clients on the SuperELAN may see a short disruption in communication while the SE spanning tree converges, depending on which ELAN they joined and to which clients they were communicating at the time of the failure.

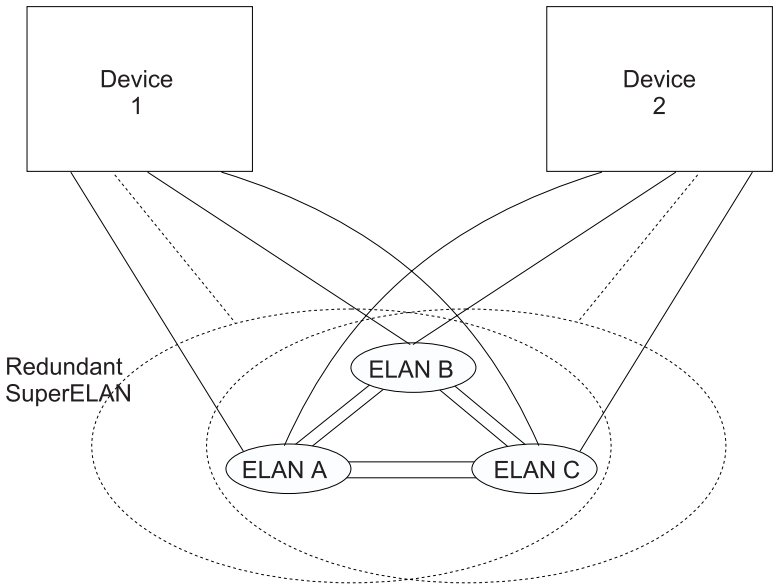


Figure 42. Redundant SuperELAN

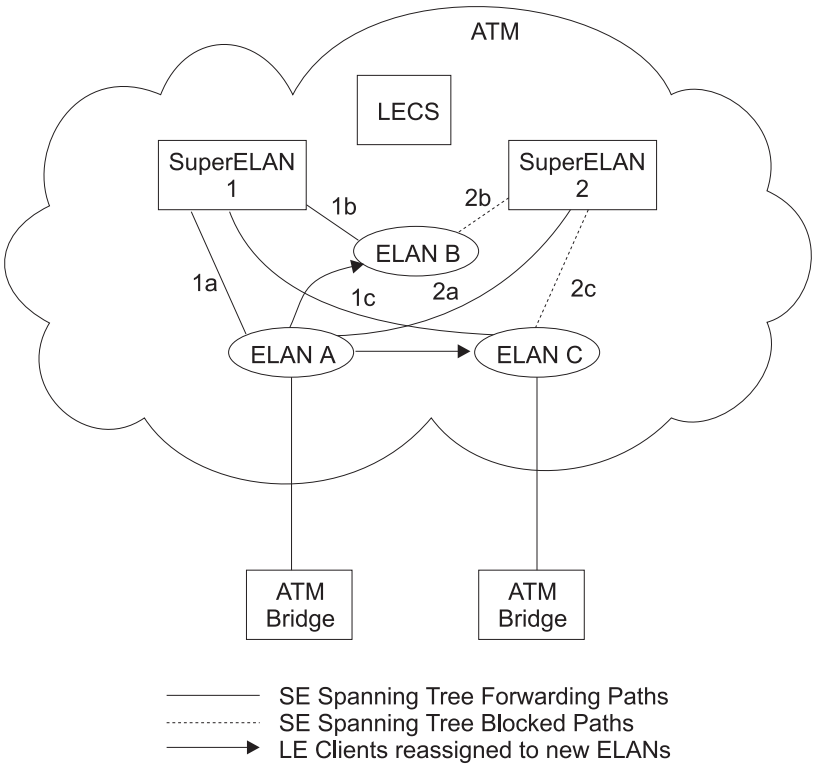


Figure 43. SuperELAN II Spanning Tree

Token Ring SuperELANs

Since the SuperELAN concept is based on grouping ELANs to form a single larger super ELAN, Token Ring SuperELANs treat the collection of ELANs as one Token

Ring segment. All bridges connected to the SuperELAN should define the SuperELAN segment as the same ring number.

The SuperELAN ring number is not configured but is learned. Once learned, specifically routed frames can be forwarded to the correct ELAN by looking up the next hop in the SuperELAN route descriptor cache. All routes and spanning tree explorer frames are transmitted to every ELAN in forwarding state (provided broadcast manager or VLAN filters have not processed the frame).

Configuring Routing Protocols on SuperELAN II Interfaces

The following routing protocols are supported on the SuperELAN II interfaces:

- IP
- IPX
- AppleTalk
- Banyan Vines

Layer-2 protocols like APPN and ASRT bridging, are not supported on SuperELAN II interfaces. If connectivity to a SuperELAN using Layer 2 protocols is needed, these protocols should be configured on non-SuperELAN II LECs and the LECs should be configured to 'join' the SuperELAN (any ELAN in the SuperELAN).

Migration to SuperELAN II

Migration from ASRT SuperELAN to SuperELAN II is provided via the **migrate** command under `SE Services>` configuration command prompt.

Once a configuration is migrated from ASRT SuperELAN to SuperELAN II, there is no automated reverse migration. Although ASRT SuperELAN and SuperELAN II can coexist within an ATM network, they can not coexist on the same device.

Sample SuperELAN II Configuration

```
Console granted to this interface
Config (only)>net 0
ATM user configuration
ATM Config>inter
ATM interface configuration
ATM Interface Config>add esi   1
ESI in 00.00.00.00.00.00 form []? 000011111111
ATM Interface Config>ex
ATM Config>le-s
LAN Emulation Services user configuration
LE Services config>les 1   2
New ELAN Name (ELANxx) []? tok1
LES-BUS configuration
LES-BUS config for ELAN 'tok1'>add
Turn on Standard Event Logging for LES [yes]
Select ELAN type
        (1) Token Ring
        (2) Ethernet

Enter Selection:  [1]?
Select ESI
        (1) Use burned in ESI
        (2) 00.00.11.11.11.11

Enter Selection:  [1]? 2

Selector x00 is generally reserved for use by the LECS,
Selector x01 is generally reserved for use by the LECS Interface.

Enter selector (in hex) [2]?
```

```
Selection "Add LES-BUS" Complete
LES-BUS config for ELAN 'tok1'>set lecid   3
Lower bound of LECID range (in hex) [1]? 100
Upper bound of LECID range (in hex) [FEFF]? 199
New LECID Range: 0x0100 through 0x0199
LES-BUS config for ELAN 'tok1'>ex


LE Services config>les 1
New ELAN Name (ELANxx) []? tok2
LES-BUS configuration
LES-BUS config for ELAN 'tok2'>add
Select ELAN type
        (1) Token Ring
        (2) Ethernet

Enter Selection:  [1]?
Select ESI
        (1) Use burned in ESI
        (2) 00.00.11.11.11.11

Enter Selection:  [1]? 2

Selector x00 is generally reserved for use by the LECS,
Selector x01 is generally reserved for use by the LECS Interface.

Enter selector (in hex) [3]?
Selection "Add LES-BUS" Complete
LES-BUS config for ELAN 'tok2'>set lecid
Lower bound of LECID range (in hex) [1]? 200
Upper bound of LECID range (in hex) [FEFF]? 299
New LECID Range: 0x0200 through 0x0299
LES-BUS config for ELAN 'tok2'>ex

LE Services config>les 1
New ELAN Name (ELANxx) []? tok3
LES-BUS configuration
LES-BUS config for ELAN 'tok3'>add
Select ELAN type
        (1) Token Ring
        (2) Ethernet

Enter Selection:  [1]?
Select ESI
        (1) Use burned in ESI
        (2) 00.00.11.11.11.11

Enter Selection:  [1]? 2

Selector x00 is generally reserved for use by the LECS,
Selector x01 is generally reserved for use by the LECS Interface.

Enter selector (in hex) [4]?
Selection "Add LES-BUS" Complete
LES-BUS config for ELAN 'tok3'>set lecid
Lower bound of LECID range (in hex) [1]? 300
Upper bound of LECID range (in hex) [FEFF]? 399
New LECID Range: 0x0300 through 0x0399

LES-BUS config for ELAN 'tok3'>ex

LE Services config>ex


ATM Config>se
SuperELAN Services User Configuration
SE Services config>add     4
SuperELAN Name []? super_tok
SuperELAN ID [0]? 88
  (  1) Ethernet
  (  2) Token-Ring
Type of SuperELAN [2]?
  (  1) 1516
  (  2) 4544
  (  3) 9234
  (  4) 18190
Maximum Frame Size of SuperELAN [2]?
SuperELAN 'super_tok' added.
```

```
SE Services config>work        5
  (  1) super_tok
  (  2) << Exit (no selection) >>
SuperELAN Name [1]?
SuperELAN 'super_tok' selected for detailed configuration.
Selected SuperELAN 'super_tok'>add     6
  (  1) << All ELANs >>
  (  2) tok1
  (  3) tok2
  (  4) tok3
  (  5) << Remote ELAN >>
  (  6) << Exit (no selection) >>
ELAN Name [1]? 1
ELAN 'tok1' added to SuperELAN 'super_tok'.
ELAN 'tok2' added to SuperELAN 'super_tok'.
ELAN 'tok3' added to SuperELAN 'super_tok'.


Selected SuperELAN 'super_tok'>list    7
------ SuperELAN Configuration -------
SuperELAN Name:          super_tok
Type:                    Token Ring
Mode:                    Enabled
Associated ATM Net       0
Frame Size:              4544
SuperELAN ID:            88

------- ELAN Cache Parameters --------
MAC Filter Cache Age:    300
MAC Filter Cache Size:   1000
RD Filter Cache Age:     1800

------ Spanning Tree Parameters ------
SuperELAN Address:       000000000000
Max Age:                 20
Hello Time:              2
Forward Delay:           15
Priority:                32768

----- Packet Tracing Parameters ------
Packet Tracing:          Disabled
Trace Dest Addr Mask:    000000000000
Trace Dest Addr Value:   000000000000
Trace Source Addr Mask:  000000000000
Trace Source Addr Value: 000000000000

----- VLAN Configuration Summary -----
                  (Enabled/Configured)
IP VLANs:                0/0
IPX VLANs:               0/0
NetBios VLANs:           0/0
Sliding Window VLANs:    0/0
Mac Address VLANs:       0/0

-------- Broadcast Management --------
IP:                      Enabled
NetBIOS Dupl. Filter:    Disabled
NetBIOS Route Caching:   Disabled


Selected SuperELAN 'super_tok'>elans      8
SuperELAN Name:          super_tok

Mode E=Enabled/D=Disabled
| SuperELAN Port Number
|    |   MSS Server Interface Number
|    |      |  ELAN Services Location
|    |      |      |    Spanning Tree Priority
|    |      |      |      |  Spanning Tree Path Cost
|    |      |      |      |    |
v    v      v      v      v    v    ELAN Name
- ----- ----- ------  --- -----  --------------------------------
```

```
E     1     1  Local  128 32768  tok1
E     2     2  Local  128 32768  tok2
E     3     3  Local  128 32768  tok3


Selected SuperELAN 'super_tok'>br       9
Enter Bridge Broadcast Manager Protocol:  IP or NetBIOS  [IP]?

IP Bridge Broadcast Manager User Configuration

IP B-BCM 'super_tok' config>ena        10
IP Bridge Broadcast Manager is   ENABLED

IP B-BCM 'super_tok' config>ex

Selected SuperELAN 'super_tok'>vlan      11

VLAN filter configuration
VLAN config>add sliding-window           12
Enter filter base (MAC or INFO) [MAC]?
Enter window filter offset (0-255) [0]? 6
Enter compare value in hex (1-10 bytes) []? 10005A000000
Enter compare mask in hex (6 bytes) [ffffffffffff]? 7fffff000000
Configure This VLAN on Specific Bridge Ports? [No]:
Age (expiration in minutes,0=infinity) [5000]?
Track Active Mac Addresses on this VLAN? [No]: y
Enable This Filter? [Yes]:
VLAN Name (Required, 32 chars max) []? IBM Mac Addresses
VLAN 'IBM Mac Addresses' (Sliding Window) successfully added


VLAN config>list sliding all             13

   --------------- SLIDING WINDOW VLANS ----------------

   Compare Value               = 0x10005A000000
   Compare Mask                = 0x7FFFFF000000
   Offset Length and Type      = 6 (MAC)
   Port  1 (Interface  1)      = Auto-Detect and Include
   Port  2 (Interface  2)      = Auto-Detect and Include
   Port  3 (Interface  3)      = Auto-Detect and Include
   Age (expiration in minutes) = 5000
   Tracking of Mac Addresses   = Enabled
   VLAN Filter State           = Enabled
   VLAN Name                   = IBM Mac Addresses
VLAN config>add mac-address              14
Configure This VLAN on Specific Bridge Ports? [No]:
Age (expiration in minutes,0=infinity) [5000]?
Track Active Mac Addresses on this VLAN? [No]:
Enable This Filter? [Yes]:
VLAN Name (Required, 32 chars max) []? Finance Dept
VLAN 'Finance Dept' (MAC Address) successfully added
VLAN config>add address                  15

Choice of Mac Address VLAN:
       VLAN Name
       =========
   (1) Finance Dept
Enter Selection [1]?
Enter New Mac Address in Hex: []? 40005A000001
New MAC Address For VLAN 'Finance Dept' successfully added
VLAN config>add address

Choice of Mac Address VLAN:
       VLAN Name
       =========
   (1) Finance Dept
Enter Selection [1]?
Enter New Mac Address in Hex: []? 40005A000002
New MAC Address For VLAN 'Finance Dept' successfully added
VLAN config>add address

Choice of Mac Address VLAN:
       VLAN Name
       =========
   (1) Finance Dept
```

```
Enter Selection [1]?
Enter New Mac Address in Hex: []? 40005A000003
New MAC Address For VLAN 'Finance Dept' successfully added


VLAN config>list mac by                16

Choice of Mac Address VLAN:
       VLAN Name
       =========
   (1) Finance Dept
Enter Selection [1]?

   ---------------- MAC ADDRESS VLAN -------------------

   Mac Address #1              = 40.00.5A.00.00.01
   Mac Address #2              = 40.00.5A.00.00.02
   Mac Address #3              = 40.00.5A.00.00.03
   Port  1 (Interface  1)      = Auto-Detect and Include
   Port  2 (Interface  2)      = Auto-Detect and Include
   Port  3 (Interface  3)      = Auto-Detect and Include
   Age (expiration in minutes) = 5000
   Tracking of Mac Addresses   = Disabled
   VLAN Filter State           = Enabled
   VLAN Name                   = Finance Dept
VLAN config>ex
Selected SuperELAN 'super_tok'>ex

SE Services config>list        17
Number of configured SuperELANS: 1

Mode E=Enabled/D=Disabled                                        BCM
| ATM Interface Net Number                                       IP
|   |  Type E=Ethernet/T=Token Ring                              | NetBIOS
|   |   |                                                        | |
v   v   v SuperELAN Name                    ID    #ELANs #VLANs v v
- ----- - -------------------------------- ----- ------ ------ - -
E     0 T                         super_tok    88      3      2 Y N
```

1 Add ESI to ATM Interface

2 Add all LES/BUSes that will be included in the SuperELAN

3 Set LEC ID range for each ELAN so that all LEC IDs in the SuperELAN will be unique

4 Add SuperELAN

5 Work on the SuperELAN

6 Add ELANs to the SuperELAN

7 List the SuperELAN configuration

8 Show the configured ELANs in the SuperELAN

9 Move to the BCM menu

10 Add IP Broadcast Management to the SuperELAN

11 Move to the VLAN menu

12 Add Sliding-Window VLAN to SuperELAN

13 List the Sliding-Window VLAN configuration

14 Add MAC-Address VLAN to SuperELAN

15 Add MAC Addresses to MAC-Address VLAN

16 List the MAC-Address VLAN

17 List summary of SuperELAN configuration

ATM Virtual Interface Concepts

An ATM Virtual Interface (AVI) creates the appearance of multiple ATM interfaces when, in fact, there is only one physical ATM interface. One or more AVIs can be configured for each physical ATM interface on the router. AVIs have the following characteristics:

- Each AVI must be defined on one (and only one) physical ATM interface. ATM real interface (ARI) will be used to mean a physical ATM interface.
- One or more AVIs can be configured on each ARI on a router.
- Higher layer protocols treat ARIs and AVIs equally. The protocols see the total number of ATM interfaces as the sum of the number of ARIs and AVIs configured on the router.
- Protocols can be configured on each ATM interface (real or virtual) independently of other interfaces.

  For example, one can configure IP on interface 0 (which is a real ATM interface) with IP address 9.1.1.1 and another instance of IP with address 9.2.1.1 on interface 1 (which is an AVI). Whether an interface is a real ATM interface or a virtual interface configured on a real interface makes no difference to the protocol (IP in the example). In addition, whether virtual interface 1 is configured on top of real ATM interface 0 or some other physical ATM interface is also transparent to the protocols.

Advantages of Using ATM Virtual Interfaces

Major advantages of using the ATM Virtual Interfaces are:

- Using the ATM Virtual Interface feature increases the number of protocol instances that can be supported on a physical ATM interface.

  The actual number of AVIs that can be configured on an ARI is limited by physical resources, such as memory, available on the router. The total number of interfaces that can be created depends on the data packet size for the interfaces and is limited to a maximum number of 253 per router.

  The use of AVIs significantly improves the configuration options for protocols such as IPX that are limited to one instance or address per ATM interface. By configuring an appropriate number of AVIs, several IPX addresses can be supported on each physical ATM interface.
- The ATM Virtual Interface feature is crucial for supporting multicast routing protocols (such as MOSPF) over ATM networks.

  In order for multicast to operate correctly, each logical subnet ***must*** be configured on a different interface because multicast routing protocols typically function in such a way that a packet coming in from a router interface will never be sent out over the same interface. Thus, if more than one subnet is configured on an interface and a source in one subnet sends a multicast packet to a member in another subnet defined on the same interface, this member will never receive the packet.

  By creating an individual virtual interface for each subnet, packet multicasting can be performed successfully. Typically, the number of ATM interfaces on a router will be limited, in turn limiting the number of subnets that can be correctly configured for multicast operation. However, by creating as many AVIs as needed (according to the number of subnets that are required to be configured on the router), the number of physical ATM interfaces will no longer limit the number of subnets that can be configured on a router for correct multicast operation.

For example, the “one-armed” router cannot support multicast traffic over interfaces other than ELANs without the AVI feature, because incoming packets will never be sent out the same interface and will be discarded instead.

- Creating multiple AVIs on an ARI and configuring each different protocol instance (for example, each IP subnet) on a different AVI on the same ARI, can improve performance.

  For example, when multiple subnets are configured on a single physical ATM interface, the interface will have to reduce the maximum transmission unit or MTU (the maximum packet size that can be sent or received over that interface) to the smallest MTU of all subnets sharing the same interface. However, if multiple AVIs are created on that ARI and each IP subnet is configured on a different AVI, every subnet can continue to use its existing MTU size without consideration of other subnets configured on the same physical ATM interface. This avoids possible reduction in throughput and delays due to packet fragmentation and reassembly caused by MTU size reduction.

  Another performance improvement can be achieved by distributing the number of protocol addresses configured on a physical interface over different virtual interfaces configured on the same physical interface. The per-interface protocol lists get shortened, resulting in faster searches and reduced processing time.

Disadvantages of using ATM Virtual Interfaces

The disadvantages of using ATM Virtual Interfaces are:

- Because AVIs do not have any physical resources of their own, each virtual interface may have fewer Virtual Connections (VCs) than a single physical interface. The available resources (in this example VCs) are partitioned among the different virtual interfaces configured on a single ARI and the ARI itself.

  In the current implementation, resource allocation is *on demand*. Each physical ATM interface has a pool of resources that are available for use by all AVIs and the single ARI itself.

Note: Because all resources are shared among the ARI and all its AVIs, an ESI added on an ARI is automatically available to all AVIs configured on the ARI. You should not assign the same ESI and selector combination to two different protocol clients using the same ARI even though they are configured on different AVIs.

Limited PVC sharing is allowed across the ARI and the AVIs configured on the ARI. PVC sharing is limited to different protocol instances. Multiple instances of the same protocol are not allowed to share the same PVC.

Chapter 20. Configuring and Monitoring ATM

This chapter describe the ATM interface configuration and operational commands. It includes the following sections:

- "Accessing the ATM Interface Configuration Process"
- "ATM Configuration Commands" on page 268
- "ATM Interface Configuration Commands" on page 269
- "SuperELAN II Configuration Commands" on page 283
- "ATM Virtual Interface Configuration Commands" on page 275
- "ATM Virtual Interface Monitoring Commands" on page 281
- "Accessing the ATM Monitoring Process" on page 276
- "ATM Monitoring Commands" on page 277
- "ATM Interface Monitoring Commands (ATM INTERFACE+ Prompt)" on page 278
- "ATM-LLC Monitoring Commands" on page 281

Accessing the ATM Interface Configuration Process

Use the following procedure to access the configuration process.

1. At the OPCON prompt, enter **talk 6**. (For more detail on this command, refer to "What is the OPCON Process?" on page 75.) For example:

   ```
   * talk 6
     Config>
   ```

   The CONFIG prompt (`Config>`) displays on the console. If the prompt does not appear when you first enter configuration, press **Return** again.

2. At the CONFIG prompt, enter the **list devices** command to display the network interface numbers for which the router is currently configured.
3. Record the interface numbers. If ATM is not specified as an interface, then create an ATM interface by using the **add device** command at the Config> prompt.

   If ATM is not specified as an interface, enter the **add device atm** command.

   ```
   Config> add dev atm
   Device Slot x(0-3) 0?
   Adding CHARM ATM Adapter device in slot 0 port 1 as interface xx
   (where xx is the interface number assigned)
   ```

   Note: You can define two ATM interfaces on an IBM 8210 Multiprotocol Switched Services Server but only one on a IBM Nways Multiprotocol Switched Services (MSS) Server Module for an 8260/8265.
4. Enter the **network** command and the number of the ATM interface you want to configure. For example:

   ```
   Config> network 0
   ATM Config>
   ```

   The ATM configuration prompt (`ATM Config>`), is displayed.

© Copyright IBM Corp. 1996, 1998

ATM Configuration Commands

This section summarizes the ATM configuration commands. Enter the commands at the `ATM config>` prompt.

Table 23. ATM Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
INTERFACE	Displays the `ATM Interface Config>` prompt from which you can list, change, or configure the ATM Interface. • Add an ESI. • List the current configuration or list ESIs. • Remove an ESI. • Set parameters of the ATM network. • Enable or disable an ESI. • Exit
LE-SERVICES	Displays the `LE Services Config>` prompt from which you can list, change, or configure LAN Emulation Services as described in “Chapter 24. Using LAN Emulation Services” on page 349 . • LECS displays the `LECS Config>` prompt from which you can configure a LAN Emulation Configuration Server. • LES-BUS displays the `LES-BUS config for ELAN 'x'>` prompt from which you can configure a LAN Emulation Server — Broadcast and Unknown Server (LES-BUS). • List all LES-BUS names. • SECURITY (LES/LECS INTERFACE TO VALIDATE JOINS) displays the `LECS Interface Config>` prompt from which you can list, change, or configure security between the LECS and LES-BUS pairs.
SE-SERVICES	Displays the `SE Services Config>` prompt from which you can list, change, or configure SuperElan Services.
LE-CLIENT	Displays the `LE Client Config>` prompt from which you can list, change, or configure the LAN Emulation Client Interface as described in “Chapter 22. Using LAN Emulation Clients” on page 311. • Add a LAN Emulation Client (LEC) for a token-ring or Ethernet emulated LAN. • Configure a LEC by network #. This command displays the `LE Config>` prompt, from which you can configure a specific LAN Emulation Client (LEC). • List LAN Emulation Clients (LECs). • Remove a LAN Emulation Client (LEC).
VIRTUAL ATM	Displays the `ATM Virtual Interface Config>` prompt from which you can list, add, or remove the ATM Virtual Interface as described in “ATM Virtual Interface Configuration Commands” on page 275
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

ATM Interface Configuration Commands

This section summarizes and then explains the commands for configuring a specific ATM interface.

Enter the commands at the `ATM INTERFACE>` prompt.

Table 24. ATM INTERFACE Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds an ESI.
List	Lists the current configuration or list ESIs.
Qos	Displays the `ATM I/F 0 QOS Config>` prompt from which you can configure Quality of Service as described in “QoS Configuration” on page 270.
Remove	Removes an ESI.
Set	Sets parameters of the ATM network.
Disable	Disables an ESI.
Enable	Enables an ESI.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to add an ESI to your ATM configuration.

Octets 14–19 of an ATM address are the End System Identifier (ESI). Each end system attached to the same switch must use a disjoint set of ESIs. When an end system activates, it attempts to register its ESIs with its ATM switch using ILMI. The switch forces all of its registered ESIs to be unique.

Syntax:

add esi *esi-address*

esi *esi-address*

Address of End System Identifier.

Valid Values: Any 12 hexadecimal digits

Default Value:

none

List

Use the **list** command to list the configuration of this ATM device or to list the set of configured ESIs.

Syntax:

list configuration

esi

configuration

Lists the ATM device configuration. For an explanation of the listed fields, see “Set” on page 270.

Example: `list con`

```
                        ATM Configuration

  Interface (net) number =     0
  Maximum VCC data rate Mbps   =      155
  Maximum frame size    = 9234
  Maximum number of callers =  209
  Maximum number of calls =  1024
  Maximum number of parties to a multipoint call =  512
  Maximum number of Selectors that can be configured  =  200
  UNI Version = UNI 3.0
  Packet trace = OFF
```

esi Lists the ESIs in the ATM configuration.

Example: `list esi`

```
ATM INTERFACE> list esi

        ESI                 Enabled
------------------------   -------
000000000009                  YES
000000000100                  YES
```

QoS Configuration

Use the **qos-configuration** command to display the `ATM I/F 0 QOS Config>` prompt from which you can configure Quality of Service as described in "QoS Configuration".

Syntax:

qos-configuration

Remove

Use the **remove** command to remove an ESI from your ATM configuration. All ATM components using this ESI should be reconfigured to use a different ESI. An ATM component that attempts to use a removed ESI may not activate on the next router restart.

Syntax:

remove esi *esi-address*

esi *esi-address*

Address of End System Identifier.

Valid Values: Any 12 hexadecimal digits

Default Value:

none

Set

Use the **set** command to specify ATM network parameters.

Syntax:

set max-data-rate

max-frame

max-config-selectors

max-calls

max-callers

max-mp-parties

trace

uni-version

network-id

max-data-rate *speed*

Sets the default and upper bound for VCC traffic parameters of most LANE and CIP connections. For example, this is the default PCR for best-effort VCCs initiated by LE Clients. Signaled SCRs and PCRs cannot exceed this limit. The default value should be satisfactory in most situations. An example of a situation where it is beneficial to change this value would be if the majority of the stations use 25–Mbps adapters. In this case, it may be desirable to limit the data rate on VCCs to 25 Mbps so that the lower speed stations are not overwhelmed with frames from the router. The units for this parameter are Mbps.

Valid Values:

25

100

155

Default Value:

155

Example:

```
ATM INTERFACE> set speed 155
```

max-calls

Sets the maximum number of switched virtual circuits (SVCs) that can exist on this ATM device. Every point-to-point and point-to-multipoint SVC uses system resources. This parameter helps limit the system resources reserved for signaling and switched connections. Increasing this parameter will allow more simultaneous SVCs. However, more system memory will be required to manage these connections.

Valid Values:

An integer in the range 64 - 10500

Default Value:

1024

Example:

```
ATM INTERFACE> set max-calls 500
```

max-callers

Sets the maximum number of entities on the router that use the ATM interface. Each LEC, LES/BUS, LECS, LECS Interface, Classical IP Client, and 1483 bridge interface qualifies as a user of the ATM interface. Increasing this parameter allows more users of the interface and uses more system memory.

Valid Values:

An integer in the range 64 – 1024

Default Value:
209

Example:

```
ATM INTERFACE> set max-callers 25
```

max-config-selectors

Sets the maximum number of selectors under your specific control.

The selector is used to distinguish different users on the same end system. VCC setup requests are routed in the following hierarchical fashion: ATM switches route to the destination ATM switch using the Network Prefix, the destination ATM switch routes to the destination end system using the ESI, and the end system notifies the destination user based on the selector.

Each ESI can have up to 255 associated selectors (0x00 through 0xff). The range of selectors is partitioned into two subranges, a configured selector range and an automatically assigned selector range. The ATM interface parameter max-configured-selector gives the upper bound on the configured selector range.

The ATM components on the router have various ways of choosing a selector. Some components require you to explicitly configure a selector from the configured selector range. LES/BUSs are an example of such a component.Other components, such as Classical IP clients, allow the selector to be automatically assigned at run-time. You do not have to choose the selector because the router does this when it activates. This selector is not guaranteed to be consistent across router restarts. Automatic selector assignment is useful only for those ATM components whose ATM address does not have to be already known by other network devices.

The relative sizes of the selector range can be modified to conform to the types and numbers of ATM users on the router.

Valid Values:
0 – 255 (0x00 – 0xFF)

Default Value:
200

Note: The selector is byte 20 of a 20-byte ATM address.

Example:

```
ATM INTERFACE> set max-config-selectors 225
```

max-frame

Sets the maximum number of octets permitted in any data frame sent or received on the ATM interface. System memory is allocated based upon this parameter. Increasing the max-frame requires more system memory, but allows processing of larger frames.

All router entities using the ATM interface must use a maximum frame size less than or equal to the max-frame-size of the ATM interface. This includes all LECs, CIP clients, and 1483 bridge interfaces.

Valid Values:
An integer in the range 512 - 31000

Default Value:
9234

Example:

```
ATM INTERFACE> set max-frame 1000
```

max-mp-parties

Sets the maximum number of leaves on a point-to-multipoint connection initiated by the router. This parameter affects system memory allocation. Increasing this value is necessary if the router must set up point-to-multipoint connection(s) to a large number of destinations.

Valid Values:

An integer in the range 1 – 5000

Default Value:

512

Example:

```
ATM INTERFACE> set max-mp-parties 300
```

trace Sets the packet tracing parameters on the interface. Packet tracing can be enabled or disabled on a range of VPI/VCI values. Common VPI/VCI values to trace are:

- 0/5 for signalling packets
- 0/16 for ILMI packets.

Valid Values:

ON or OFF

Default Value:

ON

You are prompted for the VPI/VCI range you want to trace.

Beginning VPI Valid Values:

0 – 255

Default Value:

0

Ending VPI Valid Values:

0 - 255

Default Value:

255

Beginning VCI Valid Values:

0 - 65535

Default Value:

0

Ending VCI Valid Values:

0 - 65535

Default Value:

65535

Example:

```
ATM INTERFACE> set trace on
beginning of VPI range [0]? 0
end of VPI range [255]? 0
beginning of VCI range [0]? 5
end of VCI range [65535]? 5
```

uni-version

Sets the User Network Interface (UNI) version used by the ATM interface with communicating with the attached ATM switch. If the UNI versions are configured on the ATM switch and ATM device interface to a specific version (not AUTO-DETECT), the UNI versions must match.

If the UNI version is configured as AUTO, the ATM device attempts to learn the UNI version to use from the switch.

In UNI AUTO-DETECT mode, if the switch does not respond to the query for UNI version, the default is UNI 3.0. If the switch responds with a value other than UNI 3.0 or UNI 3.1, the default is UNI 3.1.

Valid Values:

[UNI 3.0|UNI 3.1|AUTO-DETECT|None]

Default Value:

UNI 3.0

Note: Must be compatible with the ATM switch.

Example:

```
ATM INTERFACE> set uni-version 3.0
```

network-id

Sets the network id of the ATM interface. Multiple ATM interfaces should have the same network id if there is ATM connectivity between the interfaces.

Valid Values:

0 - 255

Default Value:

0

Enable

Use the **enable** command to enable an ESI in the configuration of your ATM device. The ATM interface attempts to register only enabled ESIs when it activates.

Syntax:

enable esi *esi-address*

esi *esi-address*

Address of End System Identifiers.

Valid Values:

Any 12 hexadecimal digits

Default Value:

none

Example: `enable esi`

```
ATM INTERFACE> enable esi 00:00:00:00:00:09
```

Disable

Use the **disable** command to disable an ESI in the configuration. ATM components using disabled ESIs will not become active on the next router restart.

Syntax: disable esi *esi-address*

esi *esi-address*

Address of End System Identifiers.

Valid Values:

Any 12 hexadecimal digits

Default Value:

none

Example: `disable esi`

```
ATM INTERFACE> disable esi 00:00:00:00:00:09
```

Accessing the Virtual ATM Interface Configuration Process

From the `ATM Config>` prompt of a selected real ATM interface, use the **Virtual ATM** command to enter the Virtual ATM configuration command mode.

ATM Virtual Interface Configuration Commands

This section summarizes the ATM virtual interface configuration commands. Enter the commands at the `ATM virtual interface config>` prompt.

Table 25. ATM Virtual Interface Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds a virtual ATM interface.
List	Lists the current configured virtual ATM interfaces.
Remove	Removes the virtual ATM interface from the current configuration.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to add an ATM virtual interface. A new ATM virtual interface is added to the corresponding ATM real interface (the configuration menu from which this ATM virtual interface configuration menu is accessed). The net/interface number assigned to the newly created ATM virtual interface is displayed and it is one number greater than the current largest interface number.

Syntax:

add

Example:

```
ATM Virtual Interface config> add
Added ATM Virtual Interface Net as interface 5 on physical ATM interface 0
ATM Virtual Interface config>
```

List

Use the **list** command to list configured ATM virtual interfaces defined on the current real ATM interface.

ATM Virtual Interface Configuration Commands (Talk 6)

Syntax:

list

Example:

```
ATM Virtual Interface config> list

                    ATM Virtual Interface Nets
-------------------------------------------------------------------------
  ATM interface number = 0
  ATM Virtual Interface Net interface number = 5

ATM Virtual Interface config>
```

Remove

Use the **remove** command to delete an ATM virtual interface. The virtual ATM interface on the real ATM interface with the specified interface number will be removed from the SRAM configuration records. If you do not specify an interface number, the last ATM virtual interface on this real ATM interface will be deleted. If you enter a question mark (?), all ATM virtual interfaces on the current real ATM interface will be listed and you can select from that list the interface you want to remove.

Syntax:

remove *n*

Example: **remove** 5

```
Virtual ATM 5 deleted successfully.
ATM Virtual Interface config>
```

Accessing the ATM Monitoring Process

Use the following procedure to access the ATM monitoring commands. This process gives you access to an ATM's *monitoring* process.

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, refer to "What is the OPCON Process?" on page 75.) For example:

   ```
   * talk 5
   +
   ```

   The GWCON prompt (+) is displayed on the console. If the prompt does not appear when you first enter the console, press **Return** again.

2. Enter **interface** at the + prompt to display a list of configured interfaces.
3. Record the interface numbers.
4. Enter **network** followed by the number of the ATM interface.

   ```
   + network 1
   ATM+
   ```

   The ATM monitoring prompt (ATM+) is displayed.

ATM Monitoring Commands

This section summarizes the ATM monitoring commands for monitoring ATM interfaces. Enter the commands at the ATM+ prompt.

Table 26. ATM monitoring command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Interface	Displays the ATM Interface+ prompt from which you can monitor the ATM Interface, as described in “ATM Interface Monitoring Commands (ATM INTERFACE+ Prompt)” on page 278.
le-services	Displays the LE Services+ prompt from which you can monitor LAN Emulation Services as described in “Chapter 25. Configuring and Monitoring LAN Emulation Services” on page 351.
se-services	Displays the SE Services+ prompt from which you can monitor SuperELAN Services as described in “Accessing SE-Services Monitoring Process” on page 297.
Atm-llc	Displays the ATM LLC+ prompt from which you can monitor endpoints, a set of user clients, and a set of ATM channels.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Interface

Displays the ATM Interface+ prompt, described in “ATM Interface Monitoring Commands (ATM INTERFACE+ Prompt)” on page 278.

Syntax:

interface

LE-Services

Displays the LE Services+ prompt. Refer to “Chapter 25. Configuring and Monitoring LAN Emulation Services” on page 351.

Syntax:

le-services

ATM-LLC

Displays the ATM-LLC+ prompt, described in “ATM-LLC Monitoring Commands” on page 281.

Syntax:

atm-llc

ATM Interface Monitoring Commands (ATM INTERFACE+ Prompt)

This section summarizes and then explains the commands for monitoring a specific ATM interface.

Enter the commands at the `ATM INTERFACE+` prompt.

Table 27. ATM INTERFACE monitoring command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
List	Lists ATM addresses and VCCs.
Trace	Starts/Stops packet tracing on a specified VPI/VCI range. Trace can be viewed by ELS.
Wrap	Starts/Stops a loopback test on the VCC.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to list various categories of ATM data.

Syntax:

list addresses
all
circuit
vccs
reserved-bandwidth

addresses
Lists the ATM addresses, along with a descriptive name, in use on the device.

Example:

```
ATM INTERFACE+ list addresses

                ATM Address                          Name
----------------------------------------  ------------------------------------
39999999999999000099990200000041347391804  LEC 1 'eth1'
39999999999999000099990200000041347391802  LES/BUS 'eth1'
```

all Lists all of the following:

- Addresses
- Circuit statistics
- VCCs
- Reserved Bandwidth

circuit Lists the statistics for a particular VCC by specifying the particular VCI-VPI pair. You can also specify the circuit on the command line; for example: list circuit 33.

Example:

```
ATM INTERFACE+ list circuit
VPI [0]?
VCI [32]?33
```

```
Frames transmitted   =         2  Bytes transmitted   =       216
Frames received      =         2  Bytes received      =       216
```

vccs Lists all the VCCs established by the router. The VCCs may be permanent (PVC) or switched (SVC), point-to-point or point-to-multipoint, and each is identified by a unique VPI/VCI. The trace command uses the VPI/VCI value for a VCC to perform packet tracing over a particular VCC.

Example:

```
ATM Interface+ list vccs
                              VCCs
 VPI  VCI   Hndl   Type    FrmXmt     FrmRcv     ByteXmt    ByteRcv
 --- ----- ----- ------- ---------- ---------- ---------- ----------
   0   142    17    P-MP          0          0          0          0
 Name = BUS Mcast Fwd on 'eth1'

   0   143    19    P-MP          0          0          0          0
 Name = LEC 1 (LECID 0001) Mcast Fwd 'eth1'

   0   138    13  B0-139          1          0         62          0
 Name = LEC 1 (LECID 0001) Mcast Send 'eth1'

   0   139    16  B0-138          0          1          0         62
 Name = BUS Mcast Send LECID 0001 on 'eth1'

   0   134     9    P-MP          0          0          0          0
 Name = LES Cntrl Dist on 'eth1'

   0   135    11    P-MP          0          0          0          0
 Name = LEC 1 (LECID 0001) Cntrl Dist 'eth1'

   0   130     5     P-P          2          2        216        216
 Name = LEC 1 (LECID 0001) Cntrl Dir 'eth1'

   0   131     7     P-P          2          2        216        216
 Name = LES Cntrl Dir LECID 0001 on 'eth1'

   0     5     1    SAAL       2592       2592      27380      27036
 Name = SAAL

   0    16     2    ILMI        545        544      23646      35030
 Name = ILMI

VCC Totals: 4 point-to-point, 4 point-to-multipoint
ATM Interface+
```

P-P point to point VCC

P-MP point to multipoint VCC

ILMI Interim Local Management Interface VCC

SAAL signalling VCC

Bx-y Internally bound VCC to VPI x, VCI y

Sx-y Internally spliced VCC to VPI x, VCI y

reserved-bandwidth
Lists the reserved bandwidth on the ATM Interface.

Example:

```
ATM INTERFACE+ list reserved-bandwidth
Line Rate                   : 155000 Kbps
Peak Reserved Bandwidth     : None
Sustained Reserved Bandwidth : None
```

Trace

Use the **trace** command activate packet tracing over a specified range of VPI/VCI values. You can view trace data by using ELS as described in “View” on page 203.

Syntax:

trace list
on
off

list Displays the current packet tracing options on the ATM interface.

Example:

```
ATM Interface+ trace
on | off | list []? list
Packet trace is ON
Range of VPIs to be traced:       0 -       0
Range of VCIs to be traced:      32 -      39
```

on Starts packet tracing on all active VCCs within the specified VPI/VCI range.

Example:

```
ATM Interface+ trace on
beginning of VPI range [0]?
end of VPI range [0]?
beginning of VCI range [32]?
end of VCI range [65535]? 39
```

off Stops packet tracing on all VCCs.

Example:

```
ATM Interface+ trace off
ATM Interface+ trace list
Packet trace is OFF
```

Wrap

Use the **wrap** command to perform a loopback data test on the ATM interface of the adapter. Wrap can be issued on a per VC basis by specifying VPI-VCI pairs. Data is looped back internally.

You can selectively start a wrap, stop a wrap, or display the current wrap settings.

If you stop or display a wrap, the following statistics will be displayed:

- Wrap transmits
- Wrap receives
- Wrap transmit errors
- Wrap receive errors
- Wrap receive timeouts

For display, the current wrap statistics are displayed.

For stop, the final wrap statistics are displayed.

Syntax:

wrap display
start
stop

display
Displays the current wrap settings.

start Starts the wrap procedure and specifies the VPI-VCI length of pattern and the pattern itself.

Example:

```
ATM Interface+ wrap start
VPI [0]?
VCI [32]?
wrap pattern length [32]?
Enter 32-byte wrap pattern: [ABCDEFGHIJKLMNOPQRSTUVWXYZ123456]?
```

stop Stops the wrap procedure and displays final wrap statistics.

ATM-LLC Monitoring Commands

This section explains the commands for monitoring ATM LLC multiplexing.

Enter the commands at the ATM-LLC+ prompt.

Table 28. ATM LLC Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
List	Lists various options
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to list various categories of ATM LLC monitoring data.

Syntax:

list endpoints

channels

endpoints

Lists the ATM addresses in use by protocols using the ATM-LLC multiplexing function on the device. The endpoint is displayed as the End System Identifier and the Selector.

Example: `list endpoints`

```
ATM-LLC+ list endpoints
```

channels

Lists the channels in use by protocols using the ATM-LLC multiplexing function on the device.

Example: `list channels`

```
ATM-LLC+ list channels
```

ATM Virtual Interface Monitoring Commands

Monitoring the ATM virtual interface is done using the ATM LLC monitoring commands. See “ATM-LLC Monitoring Commands” for additional information.

ATM Virtual Interface Monitoring Commands (Talk 5)

Chapter 21. SuperELAN Services

This chapter describes the SuperELAN Services configuring and monitoring commands and includes the following sections:

- "Accessing the SuperELAN II Configuration Process"
- "SuperELAN II Configuration Commands"
- "Accessing SE-Services Monitoring Process" on page 297
- "SE Services Monitoring Commands" on page 297

Accessing the SuperELAN II Configuration Process

From the `ATM Config>` prompt of a selected real ATM interface, use the **se-services** command to access the `SE Services config>` prompt for SuperELAN configuration command mode.

You can also access the `SE Services config>` prompt for SuperELAN configuration command mode by issuing the **protocol se** command from the `Config>` prompt.

SuperELAN II Configuration Commands

This section summarizes the SuperELAN configuration commands. Enter the commands at the `SE Services config>` prompt.

Table 29. SuperELAN Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
ADD	Adds a SuperELAN.
DELETE	Deletes a SuperELAN configuration.
LIST	Lists the current configured SuperELANs.
MIGRATE	Migrates older ASRT SuperELAN configurations to the current SuperELAN II operational release code level.
RENAME	Renames a SuperELAN.
WORK with SuperELAN	Allows you to work with the SuperELAN configuration.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

Add

Use the **add** command to add a SuperELAN. A new Super ELAN is added to the corresponding ATM real interface (the `ATM>` configuration menu from which this SuperELAN configuration menu is accessed).

Even though a SuperELAN is directly associated with a single ATM Adapter, a SuperELAN can span multiple ATM Adapters provided the *ATM Adapter network ID* for all ATM Adapters on which the SuperELAN resides have the same value. The *ATM Adapter network ID* is a configurable parameter which identifies the ATM network to which the ATM adapter is attached. Therefore, if two ATM Adapter interfaces are configured with different ATM network IDs, a SuperELAN can not be

© Copyright IBM Corp. 1996, 1998

configured to span both ATM interfaces since shortcut VCCs could not be established between ELANs on the two ATM networks.

Syntax:

add

Example:

```
SE Services config>add
SuperELAN Name [] super_test_elan
SuperELAN ID [1] 6
  (  1) Ethernet
  (  2) Token-Ring
Type of SuperELAN [2]
  (  1) 1516
  (  2) 4544
  (  3) 9234
  (  4) 18190
Maximum Frame Size of SuperELAN [2]
SuperELAN 'super_test_elan' added.
```

Delete

Use the **Delete** command to delete a SuperELAN. If you do not specify an SuperELAN index number, a list of configured SuperELANs will be displayed. You can select from the list the SuperELAN you want to delete.

Syntax:

delete *superelan#*

Example:

```
SE Services config>del
  (  1) << All ELANs >>
  (  2) super_eth
  (  3) << Exit (no selection) >>
SuperELAN Name [1] 3
No action taken.
```

List

Use the **list** command to list all configured SuperELANs defined on all real ATM interfaces.

Syntax:

list

Example:

```
SE Services config>list
Mode E=Enabled/D=Disabled                                        BCM
| ATM Interface Net Number                                       IP
|   |  Type E=Ethernet/T=Token Ring             Proxy LE ARP    | NetBIOS
|   |   |                                       |               | |
v   v   v SuperELAN Name                   ID   v #ELANs #VLANs v v
- ----- - -------------------------------- ----- - ------ ------ - -
E     0 T                        super_tok    88 N      3      0 N N
E     1 E                        super_eth    77 N      3      2 Y N
```

Migrate

Use the **migrate** command to migrate an existing ASRT SuperELAN configuration to the current SuperELAN II operational release code level.

The previously available SuperELAN I was based on the MSS Server ASRT bridge. The new SuperELAN II runs independently of the MSS Server ASRT bridge. MSS Server 2.0.1 supports SuperELAN I as well as SuperELAN II. However, the MSS Server can be configured as SuperELAN I or SuperELAN II, but not both. A migration utility is provided from the MSS Server console to migrate a SuperELAN I configuration to SuperELAN II.

Note: The **migrate** utility is only available from the MSS Server console and the web interface. It is not available from the MSS Server Configuration Program. If you plan to use the Configuration Program to manage MSS Server configurations:

1. Migrate the SuperELAN I configuration using the **migrate** command as described in this section
2. Retrieve the updated configuration from the MSS Server using the Configuration Program and save it as a `cdb` file.

Migration to SuperELAN II is provided via the command under the SuperELAN configuration menu. The **migrate** command will scan the ASRT bridge configuration records and migrate any ports which are enabled for SuperELAN I. You will be prompted to enter additional SuperELAN information for each ASRT port that can be migrated to SuperELAN II.

Prior to invoking the **migrate** command, you should:

1. Backup the original configuration
2. Have the following information available for each current ASRT port enabled for SuperELAN I:
   a. The ELAN which the ASRT port LEC joins
   b. The location of the ELAN relative to this MSS Server (the ELAN's LES/BUS is in this local MSS Server or in a remote MSS Server .

To migrate the existing configuration:

1. At the * prompt, enter **talk 6**.
2. At the `Config>` prompt, enter **net 0**. (if 0 is the ATM interface)
3. At the `ATM Config>` prompt, type **se-services**.
4. At the `SE Services Config>` prompt, type **migrate**.

After migration is complete, the migrated ASRT configuration records are updated and new SuperELAN records are added. Migrated changes will become effective after the new configuration is saved and the MSS Server is restarted.

Use the **migrate** command to migrate an existing ASRT SuperELAN configuration to the current SuperELAN II operational release code level.

The **migrate** command can only be invoked when an ASRT SuperELAN configuration is present. Once migrated to SuperELAN II, there is no migration path back to the ASRT SuperELAN configuration.

Syntax:

migrate

Example:

```
* talk 6
Config> net 0
ATM Config> se-services
SE Services Config> migrate
SuperELAN ID:22     SuperELAN Name: []? star backbone
SuperELAN will be added to ATM Interface Number []?
  ASRT Port:1    Ifc:1     Is Port's LEC joined to Remote ELAN? [No]:
  ELAN Name (if Local must match LES/BUS Name): []? chicago
  ASRT Port:2    Ifc:2     Is Port's LEC joined to Remote ELAN? [No]:
  ELAN Name (if Local must match LES/BUS Name):[]  tulsa
  ASRT Port:3    Ifc:3     Is Port's LEC joined to Remote ELAN? [No]: yes
  ELAN Name (if Local must match LES/BUS Name): []? baltimore

Migrate ASRT SuperELAN ID 22 to SuperELAN II 'star backbone'
  ASRT Port: 1    Interface: 1    Remote ELAN: No   ELAN Name: chicago
  ASRT Port: 2    Interface: 2    Remote ELAN: No   ELAN Name: tulsa
  ASRT Port: 3    Interface: 3    Remote ELAN: Yes  ELAN Name: baltimore

The above ASRT ports will be migrated, do you want to continue? [Yes]:
Adding SuperELAN star backbone, ID=22
SuperELAN 'star backbone' added.
ELAN 'chicago' added to SuperELAN 'star backbone'
ELAN 'tulsa' added to SuperELAN 'star backbone'
ELAN 'baltimore' added to SuperELAN 'star backbone'
Migration complete.
Please write config and reboot for migration to take effect.

SE Services Config>list
Number of configured SuperELANS: 1

Mode E=Enabled/D=Disabled                                        BCM
| ATM Interface Net Number                                      IP
|   | Type E=Ethernet/T=Token Ring            Proxy LE ARP      | NetBIOS
|   |  |                                       |                 | |
v  v  v SuperELAN Name                  ID    v #ELANs #VLANs v v
- --- - ------------------------------ ----- - ------ ------ - -
E   0 E                    star backbone    22 N      3      0 N N
SE Services Config> w
  (  1) star backbone
  (  2) << Exit (no selection) >>
SuperELAN Name [1]?
SuperELAN 'star backbone' selected for detailed configuration.

SuperELAN 'star backbone' Config> elan
SuperELAN Name:          star backbone

Mode E=Enabled/D=Disabled
| SuperELAN Port Number
|    |   MSS Server Interface Number
|    |      |  ELAN Services Location
|    |      |      |    Spanning Tree Priority
|    |      |      |      |  Spanning Tree Path Cost
|    |      |      |      |    |
v    v      v      v      v    v    ELAN Name
- ----- ----- ------  --- -----  --------------------------------
E     1     1  Local  128 32768  chicago
E     2     2  Local  128 32768  tulsa
E     3     3 Remote  128 32768  baltimore
```

Rename

Use the **rename** command to rename a SuperELAN.

Syntax:

rename

Example:

```
SE Services config>rename
  (  1) super_eth
  (  2) super_test_elan
  (  3) << Exit (no selection) >>
ELAN Name [1] 2
ELAN Name [super_test_elan] super_tok
Renamed ELAN 'super_test_elan' to 'super_tok'
```

Work with SuperELAN

Use the **Work with SuperELAN** command to select a SuperELAN for detailed configuration. Use this command to access the `Selected SuperELAN 'x'>` prompt so that you can provide detailed configuration of SuperELAN x.

Syntax:

work *superelan#*

Example:

```
  SE Services config> work
  (  1) super_eth
  (  2) super_tok
  (  3) << Exit (no selection) >>
ELAN Name [1] 2
ELAN 'super_tok' selected for detailed configuration.
```

Selected SuperELAN Configuration

This section describes the selected SuperELAN detailed configuration commands. Enter the commands at the `Selected SuperELAN 'x'>` prompt.

Table 30. Selected SuperELAN Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
ADD ELAN to SuperELAN	Adds an ELAN to a SuperELAN.
BROADCAST-MANAGER	Enters the Broadcast Manager configuration menu.
DELETE ELAN from SuperELAN	Deletes an ELAN from a Super ELAN configuration.
DISABLE SuperELAN	Disables a Super ELAN configuration.
ELANs	Lists an ELAN configuration on the selected SuperELAN.
ENABLE SuperELAN	Enables a Super ELAN configuration.
LIST	Lists the current configured SuperELAN.
SET	Sets the value of configuration parameters associated with the selected ELAN.
TRACE	Allows tracing of packets for a SuperELAN.
VLANS	Enters the VLANS configuration menu.
WORK with ELAN	Allows you to work with the selected ELAN configuration.

Table 30. Selected SuperELAN Configuration Command Summary (continued)

Command	Function
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add ELAN to SuperELAN

Use the **ADD ELAN to SuperELAN** command to add an ELAN to the selected SuperELAN.

Both local and remote ELANs may be added. Local ELANs represent LES/BUSes defined in the same device as the SuperELAN. Remote ELANs represent LES/BUSes defined in other devices.

Syntax:

add

Example:

```
Selected SuperELAN 'setest'>add

  (  1) << All ELANs >>
  (  2)  eth1
  (  3)  eth2
  (  4)  eth4
  (  5) << Remote Ethernet ELAN >>
  (  6) << Exit (no selection) >>
ELAN Name [1]? 5
Remote ELAN Name []? ext ethernet elan
Connect to remote ELAN via LECS? [Yes]: no
Remote ELAN LES Address []? 39999999999999000099990200444444555555502
ELAN 'ext ethernet elan' added to SuperELAN 'super_eth'
```

The listed ELANs are locally defined and are eligible to be added to a SuperELAN. Selecting *<< All ELANs >>* adds all listed ELANs to the selected SuperELAN. Selecting *<<Remote ELAN >>* allows you to add a remotely defined ELAN configuration to the selected SuperELAN.

Broadcast-Manager

Use the **broadcast-manager** command to access the `BBCM >` configuration prompt. Refer to the chapter entitled “Configuring Bridging” in the Multiprotocol Switched Services (MSS) Configuring Protocols and Features for additional information.

Delete ELAN from SuperELAN

Use the **Delete ELAN from SuperELAN** command to delete an ELAN from a SuperELAN configuration. All ELANs in the selected SuperELAN will be listed and you can select from that list the ELAN you want to delete.

Syntax:

delete *n*

Example:

```
Selected ELAN 'super_tok'>delete
  (  1) << All ELANs >>
  (  2) tok1
  (  3) tok2
  (  4) tok3
  (  5) << External ELAN >>
```

```
  (  6) << Exit (no selection) >>
ELAN Name [1] 2
ELAN 'tok1' deleted from to ELAN 'super_tok'.
```

Disable

Use the **disable** command to disable the selected SuperELAN.

Once the SuperELAN is started, it can be enabled from the `talk 5` monitoring menu by issuing the **enable** command from the `Selected SuperELAN 'x'` prompt. See “Enable” on page 300 for more information.

Syntax:

disable

Example:

```
Selected SuperELAN 'super_eth'>disable
SuperElan 'super_eth' is disabled.
```

ELANs

Use the **elans** command to list the configured ELANs on the selected SuperELAN.

Syntax:

elans

Example:

```
Selected SuperELAN 'super_eth'>elans
SuperELAN Name:          super_eth

Mode E=Enabled/D=Disabled
| SuperELAN Port Number
|    |   MSS Server Interface Number
|    |      |  ELAN Services Location
|    |      |      |    spanning tree Priority
|    |      |      |       |  spanning tree Path Cost
|    |      |      |       |    |
v    v      v      v       v    v    ELAN Name
- ----- ----- ------  --- -----  --------------------------------
E     1     5  Local  128 32768  eth1
E     2     6  Local  128 32768  eth2
E     3     7  Local  128 32768  eth3
```

Enable

Use the **enable** command to enable the selected SuperELAN.

Syntax:

enable

Example:

```
Selected SuperELAN 'super_eth'>enable
SuperElan 'super_eth' is enabled.
```

List

Use the **list** command to list a configured SuperELAN.

Syntax:

list

Example: `list`

```
------ SuperELAN Configuration -------
SuperELAN Name:         super_eth
Type:                   Ethernet
Mode:                   Enabled
Associated ATM Net      0
Frame Size:             1516
SuperELAN ID:           3

-------- ELAN Cache Parameters -------
MAC Filter Cache Age:   300
RD Filter Cache Age:    1800  1
Maximum MAC Cache Size: 1000

------ spanning tree Parameters ------
SuperELAN Address:      000000000000
Max Age:                20
Hello Time:             2
Forward Delay:          15
Priority:               32768

----- Packet Tracing Parameters ------
Packet Tracing:          Disabled
Trace Dest Addr Mask:    000000000000
Trace Dest Addr Value:   000000000000
Trace Source Addr Mask:  000000000000
Trace Source Addr Value: 000000000000

----- VLAN Configuration Summary -----
                   Enabled/Configured
IP VLANs:               1/1
IPX VLANs:              0/0
NetBios VLANs:          0/0
Sliding Window VLANs:   1/1
Mac Address VLANs:      0/0

-------- Broadcast Management --------
IP:                     Enabled
NetBIOS Dupl. Filter:   Disabled
NetBIOS Route Caching:  Disabled
```

Note:

1 This field does not appear for Ethernet SuperELANs.

Set

Use the **set** command to set ELAN parameters on the selected SuperELAN.

Syntax:

set address
cache age
cache size
duplicate-mac tracking
frame
proxy-le-arp

spanning

super-elan-id

Example:

```
Selected SuperELAN 'super_eth'>set ?
ADDRESS of SuperELAN spanning tree Node
CACHE
DUPLICATE-MAC Tracking
FRAME Size
PROXY-LE-ARP
SPANNING Tree Parameters
SUPER-ELAN ID
```

The following parameters can be specified with the **set** command:

address
Identifies the SE spanning tree address used for constructing the SuperELAN spanning tree.

Default Value: the lowest MAC address for all ELAN interfaces in the SuperELAN

cache This parameter sets the MAC cache age and size. For a Token-ring SuperELAN, this parameter also sets the route-descriptor cache age.

Example:

```
Selected SuperELAN 'super_tok'>set cache ?
AGE
SIZE
Selected SuperELAN 'super_tok'>set cache age
MAC Filter Cache Age (60-3600 seconds) [300]? 400
RD Filter Cache Age (600-65535 seconds) [1800]? 900
Cache Age parameters set for SuperELAN 'super_tok'.
```

duplicate-mac
This parameter allows duplicate MAC addresses to be used with port-based VLANs.

If enabled, a single MAC address may be associated with multiple ports in the SuperELAN bridge. It is recommended that this option be disabled. If enabled, you should configure Port-based VLANs to ensure that only a single copy of any MAC address is visible to any station. Extreme caution is required in the network design because duplicate MAC addresses are not generally supported in bridged environments.

Example:

```
Selected SuperELAN 'super_tok'>set duplicate-mac ?
ON
OFF
```

frame Sets the SuperELAN frame size. Only ELANs matching the SuperELAN frame size can be configured in the SuperELAN.

spanning tree parameters
Sets the SuperELAN spanning tree parameters:

Priority
Indicates the SuperELAN shortcut bridge spanning tree priority. A lower value will increase the likelihood of a SuperELAN shortcut bridge becoming the root. This value is prefixed to the SuperELAN spanning tree MAC Address to form a SuperELAN shortcut bridge ID.

Valid Values: 0 - 65535

Max age

The age at which the current spanning tree configuration is considered too old. A value that is too small may cause the spanning tree to unnecessarily re-configure. A value too large will increase the time it takes for the spanning tree to converge once an outage is detected.

Valid Values: 6 - 40

Hello Time

The interval of time, in seconds, between the generation of spanning tree configuration messages generated by the root. Lower values increase the spanning tree robustness, but increase the network traffic overhead.

Valid Values: 1 - 10

Forward Delay

The delay, in seconds, that the SuperELAN bridge waits before changing to the next port state. The forward delay should be large enough to allow all SuperELAN bridges in the SuperELAN to disable ports in the new topology prior to this shortcut bridge forwarding data frames. Values too low may cause temporary loops in the SuperELAN. Values too large may lengthen network partitions after the spanning tree has converged. The default value of 15 indicates that the shortcut bridge will begin forwarding frames 30 seconds after the spanning tree has converged: 15 seconds in listening state and 15 seconds in learning state.

Valid Values: 4 - 30

Default Value: 15

proxy-le-arp

Indicates the operational status of the SuperELAN Proxy LE ARP support. If disabled, all LE ARP requests will be forwarded onto all ELANs in the SuperELAN. If enabled, the SuperELAN will attempt to resolve the LE ARP Request first and send a LE ARP Response before flooding the LE ARP request onto all ELANs in the SuperELAN. Enabling Proxy LE ARP support uses additional memory store the learned MAC to ATM mapping, but reduces the amount of LE ARP traffic for each ELAN in the SuperELAN.

Example:

```
Selected SuperELAN 'super_tok'>set proxy-le-arp ?
ON
OFF
```

SuperELAN id

Sets the identifier associated with this SuperELAN.

Unlike the SuperELAN implementation under the `ASRT Config>` command prompt, the SuperELAN ID is used to construct redundant SuperELANs that span multiple devices. The SuperELAN ID is included as part of the spanning tree Topology frames and has external significance.

Valid Values: 1 - 65279

Trace

The **trace** command, used with the ELS packet tracing facility, controls packet tracing configuration for the SuperELAN. Issuing the **trace on** command enables

the selected SuperELAN for packet tracing. The default for packet tracing is *off*. See “Packet-trace Monitoring Commands” on page 204 for additional information.

Setting the *Destination Address Value*, *Destination Address Mask*, *Source Address Value*, and *Source Address Mask* provides a mechanism for limiting the tracing of frames sent or received by the SuperELAN bridge. Frames passing the MAC address trace filter will be forwarded to ELS to be traced. A frame is considered traceable if:

destination MAC Address of the frame ANDed with *destination address trace mask* equals the *destination address trace value*

AND

source MAC Address of the frame ANDed with *source address trace mask* equals the *source address trace value*

For example, the following trace address settings will trace any frame received or transmitted to any ELAN in the SuperELAN that has a destination address of 0x000012120021 and was originated from any device with a MAC address beginning with 0x10005A.

Trace Dest Address Mask = FFFFFFFFFFFF

Trace Dest Address Value = 000012120021

Trace Source Address Mask = FFFFFF000000

Trace Source Address Value = 10005A000000

Note: The trace mask and value settings do not effect the tracing of bridge LAN Emulation control frames.

Syntax: trace on

off

address

Example:

```
Selected SuperELAN 'super_eth'>trace on
Packet Tracing enabled for SuperELAN 'super_eth'.
```

Work with ELAN

Use the **work with ELAN** command to get to the `Selected ELAN 'x'>` prompt. At this prompt, you can provide detailed ELAN configuration parameters for this ELAN in the selected SuperELAN

Syntax:

work with ELAN *elan#*

Example:

```
Selected ELAN 'super_tok'> work
  (  1) tok1
  (  2) tok2
  (  3) tok3
  (  4) << Exit (no selection) >>
ELAN Name [1] 2
ELAN 'tok2' selected for detailed configuration

Selected ELAN 'tok2'>
```

SuperELAN Configuration Commands

See “Selected ELAN Configuration” for information about commands available at the `Selected ELAN 'x'>` prompt.

VLANs

Use the **vlans** command to access the `SuperELAN 'x'VLAN config>` configuration prompt. Refer to the chapter entitled “Configuring Bridging” in the Multiprotocol Switched Services (MSS) Configuring Protocols and Features for additional information.

Syntax:

vlans

Selected ELAN Configuration

This section summarizes the selected SuperELAN detailed configuration commands. Enter the commands at the `Selected ELAN 'x'>` prompt.

Table 31. Selected ELAN Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
DISABLE	Disables an ELAN.
ENABLE	Enables an ELAN from a Super ELAN configuration.
LIST	Lists the current configured ELAN.
LE-CLIENT Configuration	Points to the LE-CLIENT configuration menu.
LES-BUS Configuration	Points to the LES-BUS configuration menu.
SPANNING TREE PORT	Sets spanning tree port parameters.
TRACE	Controls packet tracing for the ELAN.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Disable

Use the **Disable** command to disable an ELAN. Disabling the ELAN prevents clients of the disabled ELAN from setting up shortcut Data Direct VCCs with clients on other ELANs in the SuperELAN. It does not prevent clients in the disabled ELAN from communicating with clients in other ELANs if routing has been enabled on the disabled SuperELAN interface. Also, it does not prevent clients on the disabled ELAN from setting up Data Direct VCCs among themselves.

Syntax:

disable *elan#*

Example:

```
 Selected ELAN 'super_tok'>disable
   (  1) << All ELANs >>
   (  2) tok1
   (  3) tok2
   (  4) tok3
   (  5) << Remote ELAN >>
   (  6) << Exit (no selection) >>
ELAN Name [1]:2
ELAN 'tok1' disabled
```

Enable

Use the **Enable** command to enable an ELAN on a SuperELAN configuration.

Syntax:

enable *elan#*

Example:

```
Selected ELAN 'super_tok'>enable
  (  1) << All ELANs >>
  (  2) tok1
  (  3) tok2
  (  4) tok3
  (  5) << Remote ELAN >>
  (  6) << Exit (no selection) >>
ELAN Name [1]2
ELAN 'tok1' enabled
```

LE-Client Configuration

Use the **le-client** command to move directly to the ATM LAN Emulation client configuration menu for the SuperELAN interface associated with the selected ELAN. See “Chapter 22. Using LAN Emulation Clients” on page 311 for additional information.

Syntax:

le-client

LES-BUS Configuration

Use the **les-bus** command to move directly to the LES-BUS configuration menu for the selected ELAN. See “Chapter 24. Using LAN Emulation Services” on page 349 for additional information.

This menu item is visible only for *locally* configured LAN Emulation Services.

Syntax:

les-bus

List

Use the **list** command to list configured ELANs.

Syntax:

list

Example:

```
Selected ELAN 'tok4'>list
-------- ELAN Configuration ----------
ELAN Name:                ext ethernet elan
Type:                     Token Ring
Mode:                     Enabled
Frame Size:               4544
SuperELAN ID:             35
Port Number:              1
LANE Service Location:    Remote
```

```
------ spanning tree Parameters ------
ELAN Port Priority:       128
Path Cost:                32768

-------- Interface Parameters --------
ATM Physical Interface:   0
LEC Interface Number:     1
LECS Auto Configuration:  No
LE Server ATM address:    39.99.99.99.99.99.99.00.00.99.99.02.00.44.44.44.55.55.
55.02
```

Spanning Tree Port Parameters

Use the **spanning tree port** command to set spanning tree port parameters for the selected ELAN.

Syntax:

spanning tree port	port priority
	path cost

Example:

```
Selected ELAN 'tok2'>span
ELAN Port Priority (0-255) [128] 5
ELAN Path Cost (0-65535)  [32768] 27777
SuperELAN spanning tree parameters set for ELAN 'tok2'.
```

ELAN port priority

A one-octet value which influences which ELAN is used when two or more ELANs are connected to the same network segment in a loop. A lower value represents a higher priority.

Valid Values: 0 - 255

ELAN path cost

The cost added to the root path cost in the spanning tree configuration message received on this ELAN in order to determine the path cost to get to the root SuperELAN bridge through this ELAN.

Using a small value for this parameter increases the probability that this ELAN will be close to the root SuperELAN shortcut bridge, and thus asked to carry more broadcast unknown-unicast traffic and LE control traffic.

Valid Values: 0 - 65535

Trace

The **Trace** command enables packet tracing for the selected ELAN in the SuperELAN. When used with the Packet Tracing subsystem in ELS, all frames received and transmitted for this ELAN are traced. Destination and Source MAC Address filters are provided to help limit the number of traced data frames. These trace filters are configured using the SuperELAN TRACE ADDRESS command and are applied to all ELANs in the SuperELAN. See “Packet-trace Monitoring Commands” on page 204 for more information.

Syntax:

trace	on
	off

Example:

```
Selected ELAN 'tok1'>trace ?
ON
OFF

Selected ELAN 'tok1'>trace on
Packet tracing enabled for ELAN port 'tok1' on SuperElan 'super_test_elan'.
```

Accessing SE-Services Monitoring Process

Displays the `SE Services+` prompt.

This prompt can also be accessed using the **protocol se** command from the + prompt. See “SE Services Monitoring Commands”.

SE Services Monitoring Commands

Table 32. SE Services Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
CREATE	Dynamically creates and starts a newly configured SuperELAN without rebooting the device.
LIST	Displays information about the current configuration.
WORK with SuperELAN	Displays the `Selected SuperELAN 'x'` prompt from which you can monitor SuperELAN Services.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Create

Use the **Create** command to create a new SuperELAN.

Syntax:

create *superelan name*

SuperELAN name
Specifies the name of the SuperELAN to be created.

Note: The SuperELAN must not be currently running and must have an associated SRAM record. One spare interface per ELAN in the SuperELAN must be available. See “Configuring Spare Interfaces” on page 88 for information about spare interfaces.

Example:

```
SE Services console>create
SuperELAN Name []? super_eth
SuperELAN interface 5 activated successfully.
SuperELAN interface 6 activated successfully.
SuperELAN interface 7 activated successfully.

SuperELAN 'super_eth' started.
```

List

Use the **list** command to display SuperELANs.

Syntax:

list

Example:

```
SE Services console>list
Number of SuperELANS: 2                                          BCM
Mode E=Enabled/D=Disabled                 Proxy LE ARP           IP
| Type E=Ethernet/T=Token-Ring             |                    | NetBIOS
| |                                        |  ELANs   VLANs     | |
v v SuperELAN Name                     ID   v Act/Cfg Act/Cfg v v     Up-time
- - ------------------------------ ----- - ------- ------- - - -----------
E T                         super_tok    88 Y 2/  3   1/  1   Y N 00.00.27.72
E E                         super_eth    77 N 3/  3   2/  2   N N 00.00.27.73
```

Work with SuperELAN

Use the **Work with SuperELAN** command to access the `Selected SuperELAN 'superelan name'>` prompt for detailed monitoring.

Syntax:

work *superelan#*

Example:

```
SE Services console>work
  (  1) setest
  (  2) super_eth
  (  3) << Exit (no selection) >>
SuperELAN Name [1]?  2
SuperELAN 'super_eth' selected for detailed console montoring.
```

See “Selected SuperELAN Monitoring Commands”for information about the commands that are available after issuing the **work** command:

Selected SuperELAN Monitoring Commands

The following commands are available at the `Selected SuperELAN 'superelan name'>` monitoring prompt:

Table 33. Selected SuperELAN monitoring command Summary

Command	Function
BROADCAST-MANAGER	See the chapter entitled “Monitoring Bridging” in the Multiprotocol Switched Services (MSS) Configuring Protocols and Features for information.
CLEAR counters	Resets counters.
CREATE	Creates an ELAN.
ENABLE	Enables the selected SuperELAN.
DISABLE	Disables the selected SuperELAN.
DISPLAY Counters	Displays counters of all ELANs in the SuperELAN.
ELANs	Lists ELANs in the SuperELAN.
FLUSH	Flushes the data on the LE control frame cache.
LIST	Displays the configured SuperELANs.
RESTART	Restarts a disabled SuperELAN.

Table 33. Selected SuperELAN monitoring command Summary (continued)

Command	Function
SET	Sets SuperELAN cache age and size.
SHOW cache	Displays the data on the LE control frame cache.
TRACE	Enables packet tracing for the selected SuperELAN.
WORK with ELAN	Displays the `Selected ELAN 'elan name'>` prompt from which you can monitor ELAN Services.
VLANs	See the chapter entitled “Monitoring Bridging” in the Multiprotocol Switched Services (MSS) Configuring Protocols and Features for information.
Exit	Exits the SE Services monitoring process and returns to the `SE Services+` monitoring prompt.

Broadcast Manager

Use the **Broadcast-Manager** command to access the Bridge Broadcast Manager monitoring prompt. Refer to the chapter entitled “Monitoring Bridging” in the Multiprotocol Switched Services (MSS) Configuring Protocols and Features for additional information.

Clear

Use the **clear** command to reset counters for all ELANs in the SuperELAN.

Syntax:

clear

Create

Use the **create** command to create and start a new ELAN. The ELAN must have been previously configured for the selected SuperELAN under `talk 6` and the ELAN can not be currently active. There must be at least one available spare interface for the ELAN. Use the **CONFIGURATION** command from the + prompt to determine the number of available spare interfaces.

Syntax:

create *elan name*

Example:

```
SE Services console>create
ELAN Name []? eth4
ELAN interface 8 activated successfully.

ELAN 'eth4' started.
```

Disable

Use the **disable** command to disable the selected SuperELAN.

Disabling the SuperELAN prevents new inter-ELAN shortcut VCCs from being established between ELANs. It does not prevent clients from setting up data direct VCCs within an ELAN and it does not disconnect inter-ELAN data direct VCCs already established.

Disabling the SuperELAN moves all spanning tree ELAN states to *Configured*. See “ELANs” for a description.

Syntax:

disable

Example:

```
Selected SuperELAN 'super_eth'>disable
SuperELAN 'super_eth' disabled.
```

Display

Use the **Display** command to display counter information for all ELANs in the SuperELAN.

Syntax:

display

See “Display” on page 306 for an example of the **display** command.

Enable

Use the **enable** command to enable the specified SuperELAN. Enabling the SuperELAN moves all spanning tree states to *listening* state. See “ELANs” for a description.

Syntax:

enable

Example:

```
Selected SuperELAN 'super_eth'>enable
SuperELAN 'super_eth' enabled.
```

ELANs

Use the **ELANs** command to display information about all the ELANs in the specified SuperELAN.

Syntax:

elans

Example:

```
Selected SuperELAN 'super_eth'>elans
SuperELAN Name: super_eth
Number of ELANS: 3            Routing
Interface Number              IP        Port Number (Dec)
   |    L=Local/R=Remote ELAN  |IPX       |    Port Priority (Hex)
   |    | E=Enabled/D=Disabled | |AT      |    |
   |    | |                    | | |BV    |    |
   |    | |                    | | | |    |    |
   |    | |                    | | | |    |    |    Last STP  Time Since
  v    v v ELAN Name           v v v v    v    v    Status    State Change
----- - - --------------------------  ---- --  ----------- ------------
    4 L E      eth1           x x . .     1 80  Forwarding  00.01.42.00
    5 L E      eth2           x x . .     2 80  Forwarding  00.01.42.04
    6 L E      eth3           . . x .     3 80  Forwarding  00.01.42.08
```

ELAN status values:

Forwarding
SuperELAN is forwarding LE control and data frames to this ELAN

Learning
SuperELAN is receiving data frames for the purpose of caching MAC addresses and Route Descriptors, but no frames are being sent to this ELAN

Listening
SuperELAN is listening for SE Spanning Tree frames to determine if this ELAN should proceed to the Learning state or Block itself

Blocked
No frames are being sent or received since another shortcut SuperELAN path exists with higher priority to this ELAN

Configured
ELAN interface is configured within the SuperELAN but is not participating in the SE Spanning Tree and is not receiving or forwarding frames. Most likely the ELAN has been disabled

NetDown
LAN Emulation interface is down, usually indicates that the LEC has not successfully joined the ELAN

Configuring
ELAN interface is initializing and will enter the Listening state (if enabled) or Configured state (if disabled) after initialization is complete

NotSetup
ELAN interface is not defined

Flush

Use the **flush** command to clear the control and/or data cache for all ELANs in the SuperELAN.

Syntax:

flush

Example:

```
Selected SuperELAN 'super_eth'>flush ?
CONTROL Frame Forwarding Cache
DATA Frame Forwarding Cache


Selected SuperELAN 'super_eth'>flush control
Control Frame Forwarding Cache flushed for SuperELAN 'super_eth'.
```

List

Use the **List** command to display the status of the selected SuperELAN.

Syntax:

list

Example:

Selected SuperELAN monitoring commands

```
Selected SuperELAN 'super_eth'>list
------ SuperELAN Configuration -------
SuperELAN Name:              super_eth
Type:                        Ethernet
Mode:                        Enabled
ID:                          44
Frame Size:                  1516

--------- ELAN Cache Status ----------
Proxy LE ARP Support:        Disabled
Duplicate MAC Tracking:      Disabled
Learned ring segment (hex):  0
MAC Cache Age:               300
MAC Cache Size:              1000
Dynamic MAC Entries Count:   5

-------- Spanning Tree Status --------
Bridge Priority-ID:          32768-000413473679
Designated Root Priority-ID: 32768-000413473679
Root Port:                   Self
Max Age:                     20
Hello Time:                  2
Forward Delay:               15
Topology Change Detected:    No
Topology Change:             No

------- Packet Tracing Status --------

Packet Tracing:              Disabled
Trace Dest Address Mask:     000000000000
Trace Dest Address Value:    000000000000
Trace Source Address Mask:   000000000000
Trace Source Address Mask:   000000000000

----- VLAN Configuration Summary -----
                    Enabled/Configured
IP VLANs:                1/1
IPX VLANs:               0/0
NetBios VLANs:           0/0
Sliding Window VLANs:    1/1
Mac Address VLANs:       0/0
Port-based VLANs:        0/0

-------- Broadcast Management --------
IP:                      Enabled
NetBIOS Dupl. Filter:    Disabled
NetBIOS Route Caching:   Disabled
```

Restart

Use the **restart** command to restart the SuperELAN. Restarting the SuperELAN causes the configuration record parameters to be used upon restart, instead of just enabling the ELAN, which restarts the ELAN with current run-time parameters. The SuperELAN must be disabled prior to issuing the **restart** command.

Syntax:

restart

Set Cache

Use the **set cache** command to dynamically set the data cache characteristics for the selected SuperELAN.

The cache age value determines the amount of time in seconds a newly added entry will remain in the cache without being re-validated.

The cache size limits the number of MAC addresses cached to prevent excessive heap usage.

Note: Route descriptor cache entries are not bound by any configurable cache limit.

Once the cache is full, the next new MAC entry added will cause the oldest MAC entry to be deleted from the cache.

Syntax:

set cache *age*
size
duplicate-mac-tracking
proxy-le-arp

Example:

```
Selected SuperELAN 'super_eth'>set cache ?
AGE
SIZE
DUPLICATE-MAC-Tracking
PROXY-LE-ARP

Selected SuperELAN 'super_eth'>set cache size
MAC Filter Cache Size (1-10000) [1000]? 2000
Cache Size parameter updated for SuperELAN 'super_eth'.
```

Show

Use the **show** command to display data or control frame cache for all ELANs in the selected SuperELAN.

Syntax: show *control*
data
duplicate-mac
dynamic-mac
registered-mac
route-descriptor **1**

1 This menu item does not appear for Ethernet SuperELANs.

Example:

```
Selected SuperELAN 'super_eth'>show ?
CONTROL Frame Forwarding Cache
DATA Frame Forwarding Cache

Selected SuperELAN 'super_eth'>show data dyn

ELAN Name                       Count MAC Address   TTL
------------------------------- ----- ------------ ----
                           eth1     1 000044891323  240
                           eth2     2 000064432998  120
                                      000099213011  300
                           eth3     0
```

Trace

Use the **trace** command to start packet tracing for the selected SuperELAN. When used with the Packet Tracing subsystem in ELS, all frames received and transmitted onto this SuperELAN are traced. Destination and Source MAC Address

filters are provided to help limit the number of traced data frames. Trace filters are configured using the SuperELAN **TRACE ADDRESS** command and are applied to ELANs in the SuperELAN. See “Packet-trace Monitoring Commands” on page 204 for more information.

Syntax:

trace	on
	off
	address

Example:

```
Selected SuperELAN 'super_eth'>trace ?
ON
OFF
ADDRESS

Selected SuperELAN 'super_eth'>trace addr
Enter dest MAC addr trace mask in xx.xx.xx.xx.xx.xx form [00.00.00.00.00.00]?
fffffffffff
Enter dest MAC addr trace value in xx.xx.xx.xx.xx.xx form [00.00.00.00.00.00]?
00005a000001
Enter source MAC addr trace mask in xx.xx.xx.xx.xx.xx [00.00.00.00.00.00]?
fffffffffff
Enter source MAC addr trace value in xx.xx.xx.xx.xx.xx [00.00.00.00.00.00]?
00005a000002
Address trace parameters updated for SuperELAN 'super_eth'.
```

Configuring the MAC mask and values as shown will allow only frames with a destination MAC address of 00005a000001 and a source MAC address of 00005a000002 to be traced. Filtering does not effect tracing of LE Control frames forwarded between SuperELAN ports.

Work with ELAN

Use the **work with ELAN** command to get to the `Selected ELAN 'elan name'>` monitoring prompt. At this prompt, you can monitor detailed ELAN parameters for the selected ELAN on the SuperELAN.

Syntax:

work with ELAN	*elan#*

Example:

```
Selected SuperELAN 'super_tok'>work
  (  1) eth1
  (  2) eth2
  (  3) eth3
  (  4) << Exit (no selection) >>
ELAN Name [1] 2
ELAN 'eth2' selected for detailed console monitoring

Selected ELAN 'tok2'>
```

See “Selected ELAN Monitoring Commands” on page 305 for information about the commands available after you issue the **work** command.

VLANs

Use the **vlans** command to access the `SuperELAN 'x' VLANs>` monitoring prompt. At this point, you can configure and monitor VLANs on this SuperELAN. Refer to the

chapter entitled “Monitoring Bridging” in the Multiprotocol Switched Services (MSS) Configuring Protocols and Features for additional information.

Syntax:

vlans

Selected ELAN Monitoring Commands

This section summarizes the selected ELAN detailed monitoring commands for a selected SuperELAN. Enter the commands at the `Selected ELAN 'x'>` prompt.

Note: Many of the commands at this prompt level perform the same action as the corresponding command at the `Selected SuperELAN 'x'>` command prompt level. The difference is that the action at this command prompt level is directed to an ELAN rather than a SuperELAN.

Table 34. Selected ELAN Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
CLEAR	Clears counters for selected ELAN.
DISABLE	Disables an ELAN.
DISPLAY	Lists the current configured ELAN counters.
ENABLE	Enables an ELAN.
FLUSH	Flushes the control or data cache associated with the ELAN.
LEC	Points to the LE-CLIENT monitoring menu.
LES-BUS	Points to the LES-BUS monitoring menu.
LIST	Lists the current configured ELAN.
RESTART	Restarts the ELAN using configuration parameters.
SHOW	Displays LE control or data cache MAC and Route Descriptor entries.
TRACE	Configures tracing for selected ELAN.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Disable

Use the **Disable** command to disable an ELAN. Disabling the ELAN prevents clients of the disabled ELAN from setting up shortcut Data Direct VCCs with clients on other ELANs in the SuperELAN. It does not prevent clients in the disabled ELAN from communicating with clients in other ELANs if routing has been enabled on any of the SuperELAN interfaces. Also, disabling the ELAN does not prevent clients on the disabled ELAN from setting up Data Direct VCCs among themselves.

Syntax:

disable *elan#*

Example:

```
Selected ELAN 'the2'>disable
 (  1) << All ELANs >>
 (  2) eth1
 (  3) eth2
 (  4) eth3
```

```
  (  5) << External ELAN >>
  (  6) << Exit (no selection) >>
ELAN Name [1]: 3
ELAN 'eth2' disabled
```

Display

Use the **Display** command to display counters for the selected ELAN.

Syntax:

display

Example:

```
Selected ELAN 'eth2'>display
SuperELAN: super_eth
-------------------------------------------------------------------------------
ELAN: eth2
---------------------------------------.---------------------------------------
Data Packet Counters                   | LE Control Frame Counters
---------------------------------------|---------------------------------------
Pkts received . . . . . .          0   | LE Control Frame received .         0
Pkts transmitted. . . . . .        0   | LE Control Frame xmitted. .         0
*Pkts disc, src addr filt. .       0   | LE Ctl disc, rcv port !fwd.         0
Pkts disc, dest addr filt .        0   | LE Ctl disc, xmit port !fwd         0
*Pkts disc, protocol filt. .       0   | ARP Requests received . . .         0
Pkts disc, rcv port !fwd. .        0   | ARP Requests transmitted. .         0
Pkts disc, rcv port no bufs        0   | ARP Requests disc, error. .         0
Pkts disc, rcv port q over.        0   | ARP Requests filt . . . . .         0
Pkts disc, xmit port !fwd .        0   | ARP Replies received. . . .         0
Pkts disc, xmit error . . .        0   | ARP Replies transmitted . .         0
Pkts disc, frame too big. .        0   | ARP Replies disc, error . .         0
Pkts disc, rif seg mismatch        0   | NARP Requests received. . .         0
*Pkts disc, rif seg dup. . .       0   | NARP Requests transmitted .         0
Pkts routed, not SEed . . .        0   | Flush Requests received . .         0
                                       | Flush Requests transmitted.         0
BPDUs received  . . . . . .        0   | Flush Replies received. . .         0
BPDUs disc, rcv port q over        0   | Flush Replies transmitted .         0
                                       | LE Ctl disc, ctl frm q over         0
```

* These counters are currently not maintained and will always be set to 0.

Enable

Use the **Enable** command to enable the selected ELAN.

Syntax:

enable *elan#*

Example:

```
Selected ELAN 'super_tok'>enable
  (  1) << All ELANs >>
  (  2) tok1
  (  3) tok2
  (  4) tok3
  (  5) << External ELAN >>
  (  6) << Exit (no selection) >>
ELAN Name [1] 2
ELAN 'tok1' enabled
```

Flush

Use the **Flush** command to clear the control and/or data cache for the selected ELAN.

Syntax:

flush control
data

Example:

```
Selected ELAN 'eth2'>flush ?
CONTROL Frame Forwarding Cache
DATA Frame Forwarding Cache


Selected ELAN 'eth2'>flush data
Data Frame Forwarding Cache flushed for ELAN 'eth2'.
```

LEC

Use the **lec** command to jump directly to the ATM LAN Emulation client monitoring menu for the SuperELAN interface associated with the selected ELAN. See “Chapter 22. Using LAN Emulation Clients” on page 311 for additional information.

Syntax:

lec

Example:

```
Selected ELAN 'eth2'>lec
ATM Emulated LAN Console
LEC+
```

LES-BUS

Use the **les-bus** command to jump directly to the LES-BUS monitoring menu for the selected ELAN. See “Chapter 24. Using LAN Emulation Services” on page 349 for additional information.

This menu item is visible only for locally configured LAN Emulation Services.

Syntax:

les-bus

Example:

```
Selected ELAN 'eth2'>les
EXISTING LES-BUS 'eth2'+
```

List

Use the **list** command to list configuration for the selected ELAN.

Syntax:

list

Example:

```
Selected ELAN 'tok4'>list
--------- ELAN Configuration ---------
ELAN Name:                          eth2
Status:                             Enabled
Location:                           Local
```

Selected ELAN monitoring commands

```
Interface Number:                 5
Port Number:                      2
Packet Tracing:                   Disabled

-------- Spanning Tree Status --------
STP State:                        Forwarding
Time Since Last STP State Change: 00.00.39.67
Spanning Tree Priority:           128
Path Cost:                        32768
Designated Root:                  000413473679
Root Cost:                        0
Designated Bridge:                000413473679
Designated Port:                  2
```

Restart

Use the **restart** command to restart the ELAN using the configuration parameters. The ELAN must be disabled prior to issuing this command.

Syntax:

restart

Example:

```
Selected ELAN 'eth1'>restart
Restarting ELAN 'eth1'.
```

Show

Use the **Show** command to display the data and control frame cache for the selected ELAN.

Syntax:

show *control*

data

dynamic-mac

registered-mac

route-descriptor **1**

1 This menu item does not appear for Ethernet SuperELANs.

Example:

```
Selected ELAN 'eth2'>show ?
CONTROL Frame Forwarding Cache
DATA Frame Forwarding Cache

Selected ELAN 'eth2'>show data ?
DYNAMIC-MAC
REGISTERED-MAC

ELAN Name                       Count MAC Address   TTL
------------------------------- ----- ------------ ----
                           eth2     2 000064432998  120
                                      000099213011  300
```

Trace

The **Trace** command enables packet tracing for the selected ELAN in the SuperELAN. When used with the Packet Tracing subsystem in ELS, all frames

received and transmitted onto this ELAN are traced. Destination and Source MAC Address filters are provided to help limit the number of traced data frames. These trace filters are configured using the **TRACE ADDRESS** command and are applied to all ELANs in the SuperELAN. See “Packet-trace Monitoring Commands” on page 204 for more information.

Syntax:

trace	off
	on

Example:

```
Selected ELAN 'eth2'>trace ?
ON
OFF

Selected ELAN 'eth2'>trace on
Packet tracing enabled for ELAN port 'eth2' on SuperElan 'super_test_elan'.
```

Selected ELAN monitoring commands

Chapter 22. Using LAN Emulation Clients

This chapter describes LAN Emulation Clients (LECs). It includes the following sections:

- "LAN Emulation Client Overview"

LAN Emulation Client Overview

As a pioneer of ATM technology, IBM defined one of the early LAN Emulation architectures. The ATM Forum LAN Emulation Specification diverged from IBM's architecture in a number of ways. IBM, like several other vendors, now has products that implement two different LAN Emulation architectures: earlier products implement the IBM LAN Emulation Architecture, while more recently developed products implement the ATM Forum LAN Emulation Specification. The MSS Server implements LE Clients for both architectures, but LE Servers for ATM Forum LAN Emulation only.

Although ATM Forum LAN Emulation is the strategic direction for multi-vendor interoperability, customers that have installed products implementing the IBM LAN Emulation Architecture must also be supported. These customers will generally fall into one of the following two categories:

1. Those who wish to continue using IBM LAN Emulation, which offers some technical advantages relative to the ATM Forum LAN Emulation
2. Those who wish to migrate to ATM Forum LAN Emulation.

The 8210 can provide routing and bridging services that support any combination of ATM Forum or IBM LAN Emulation clients. From routing and bridging perspectives, IBM LECs are functionally equivalent to ATM Forum LECs; both provide emulated Ethernet and Token-Ring interfaces with operational characteristics of real interfaces. Configure a LEC to be either of these types:

- Ethernet
  - ATM Forum-Compliant
  - IBM
- Token-Ring
  - ATM Forum-Compliant
  - IBM

LECs are equivalent to "ports" or "interfaces" on traditional routers and bridges. The router bridges and routes traffic between ports by receiving and transmitting traffic through its LECs.

There are two levels to the configuration menus for LE Clients:

1. `LE Client Config>` permits you to view the set of LE Clients on a particular ATM interface, to add or remove LECs from this set, or to enter into a more detailed configuration environment for any member of this set (see LEC commands in the following). The commands for this prompt level are described in "Configuring LAN Emulation Clients" on page 313.
2. `Token-Ring-Forum Compliant LEC Config>`, `Token-Ring-IBM LEC Config>`, `Ethernet Forum Compliant LEC Config>`, or `Ethernet-IBM LEC Config>` permits you to configure all parameters for a particular LE Client. The commands

© Copyright IBM Corp. 1996, 1998

available at this level are described in “Configuring an ATM Forum-Compliant LE Client” on page 315 and “Configuring an IBM LE Client” on page 330.

Chapter 23. Configuring and Monitoring LAN Emulation Clients

This chapter describes how to configure LAN Emulation Clients (LECs). It includes the following sections:

- "Configuring LAN Emulation Clients"
- "Configuring an ATM Forum-Compliant LE Client" on page 315
- "Configuring an IBM LE Client" on page 330
- "Accessing the LEC Monitoring Environment" on page 337
- "LEC Monitoring Commands" on page 338

Configuring LAN Emulation Clients

This section explains the commands for viewing, changing, and using the set of LE Clients on a particular ATM interface.

Enter the commands at the `LE Client Config>` prompt under the `ATM Config>` prompt, as described in "ATM Configuration Commands" on page 268.

To get to the `LE Client Config>` prompt, enter **le-c** at the ATM Config> prompt as described in "ATM Configuration Commands" on page 268.

Table 35. LAN EMULATION Client Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Add	Adds a LEC for the following types of Emulated LANs architectures: • Ethernet – ATM Forum-Compliant – IBM • Token-Ring – ATM Forum-Compliant – IBM
Config	Gets you to the `LEC Config>` prompt, from which you can configure a specific LAN Emulation Client as described in: • "Configuring an ATM Forum-Compliant LE Client" on page 315 • "Configuring an IBM LE Client" on page 330
List	Lists the LECs
Remove	Removes a LEC.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

Add

Use the **add** command to add an ATM Forum-compliant or IBM LEC for a Token-Ring or Ethernet emulated LAN.

Syntax:

© Copyright IBM Corp. 1996, 1998

add ethernet forum
ethernet ibm
token-ring forum
token-ring ibm

token-ring forum
Token ring ATM Forum compliant LEC.

Example:

```
LE Client Config> add token-ring forum
Added device as interface 3
```

token-ring ibm
Token ring IBM LEC.

Example:

```
LE Client Config> add token-ring ibm
Added device as interface 3
```

ethernet forum
Ethernet Forum-Compliant LEC.

Example:

```
LE Client Config> add ethernet forum
Added device as interface 2
```

ethernet ibm
Ethernet IBM LEC.

Example:

```
LE Client Config> add ethernet ibm
Added device as interface 1
```

Config

Use the **config** command to get you to the LEC Config> prompt, from which you can configure the details of a specific LAN Emulation Client. Refer to “Configuring an ATM Forum-Compliant LE Client” on page 315 or “Configuring an IBM LE Client” on page 330.

Syntax:

config interface#

interface#
An integer number assigned by the router when the LEC was added to the configuration. Use the **list** command to determine the interface number assigned to the LEC.

Example:

```
LE Client Config> config 3
```

List

Use the **list** command to list the LAN emulation clients.

Syntax:

list

Example:

```
LE Client Config> list
                  ATM Emulated LANs
-----------------------------------------------------
  ATM interface number = 0
  LEC interface number = 1
  Emulated LAN type    = Ethernet Forum Compliant
  Emulated LAN name    =
```

Remove

Use the **remove** command to remove a LEC.

Syntax:

remove interface#

interface#

You must specify the interface number that was assigned when the LEC was added to the configuration. Use the **list** command to determine the interface number assigned to the LEC.

Configuring an ATM Forum-Compliant LE Client

Use this process to access the appropriate `LEC Config>` prompt.:

1. Use the **config** command at the `LE Client Config>` prompt to access the appropriate LEC interface number, or use the **network** configuration command with the appropriate LEC interface number.
2. Enter the appropriate commands at either the `Ethernet Forum Compliant LEC Config>` prompt or the `Token Ring Forum Compliant LEC Config>` prompt. Commands in the following table apply to both Token-Ring and Ethernet LECs except where indicated.

This section explains the commands for configuring an ATM Forum-compliant LAN Emulation Client.

Table 36. LAN Emulation Client Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
ARP-Configuration	Allows you to configure the LE-ARP configuration for the ATM Forum-compliant client
Frame	Sets the NetWare IPX encapsulation type.
IP-Encapsulation	Sets the IP encapsulation as Ethernet (type X’0800’) or IEEE (802.3 with SNAP). Applies only to Ethernet LECs.
List	Lists the LAN Emulation Client configuration.
LLC	Accesses the `LLC Config>` configuration prompt for Token Ring LECs.
QoS-Configuration	Gets you to the `elan-x LEC QoS Config>` prompt from which you can configure Quality of Service as described in “LE Client QoS Configuration Commands” on page 480.
RIF-Timer	Sets the maximum amount of time that information in the RIF is maintained before it is refreshed. Applies only to Token-Ring LECs.
Set	Sets the LAN Emulation Client parameters.
Source-routing	Used to enable or disable source-route bridging. Applies only to Token-Ring LECs.

Table 36. LAN Emulation Client Configuration Commands Summary (continued)

Command	Function
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

ARP Configuration

Use the **arp-configuration** command to configure the static LE-ARP entries for the ATM forum-compliant LAN Emulation Client.

Syntax:

arp-configuration

Example:

```
Token Ring Forum Compliant LEC Config> arp-configuration
ATM LAN Emulation Clients ARP configuration
```

Table 37. ATM LAN Emulation Client ARP Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds an LE-ARP cache entry using a MAC or route descriptor ARP.
Config	Sets cache entry QoS parameter values.
List	Lists configured ARP cache entries.
Remove	Removes an ARP cache entry.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to add an ARP cache entry using the MAC address or a route descriptor.

MAC addresses, and route descriptors are entered as strings of hexadecimal characters with or without optional separator characters between bytes. Valid separator characters are dashes (–), periods (.), or colons (:).

Syntax:

add mac

route-descriptor

Example 1:

```
ARP config for LEC>add mac
MAC address of LE ARP Entry []? 123456789098
ATM address in 00.00.00.00.00.00:... form []? 390f00000000000000000000000000123456789098
Destination Type -  REMOTE or LOCAL [Remote]?
```

Example 2:

```
ARP config for LEC>add route 12.34
ATM address in 00.00.00.00.00.00:... form []? 390f00000000000000000000001234567890988888
ARP config for LEC>
```

Config

Use the **Config** command to configure the permanent ARP cache entry QoS parameters for the ATM forum-specific LAN Emulation Client.

Syntax:

config *arp-entry-number*

Example:

```
ARP config for LEC> config
ARP entry number [1]
Configure LEC ARP entry
```

Table 38. ATM LAN Emulation Client ARP Config Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Set	Sets QoS parameter values.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Set:

Use the **Set** command to configure the permanent ARP cache entry QoS parameters for the ATM forum-specific LAN Emulation Client.

Syntax:

set max-reserved-bandwidth
traffic-type
peak-cell-rate
sustained-cell-rate
qos-class
max-burst-size

Example:

```
ARP entry 'identifier' config> set ?
 MAX-RESERVED-BANDWIDTH
 TRAFFIC-TYPE
 PEAK-CELL-RATE
 SUSTAINED-CELL-RATE
 QOS-CLASS
 MAX-BURST-SIZE
```

See “Chapter 26. Configuring and Monitoring Quality of Service (QoS)” on page 473 for detailed information about the QoS parameters.

List

Use the **list** command to display information about ARP configuration.

Remove

Use the **remove** command to remove an configured MAC address or Route Descriptor LE-ARP entry.

Select the ARP entry number to be removed from the list provided.

Syntax:

remove *arp-entry-number*

Frame

Use the **frame** command to set the NetWare IPX encapsulation type. The command options differ depending on the type of LEC (Token-Ring or Ethernet). For Token-Ring LECs, enter one of the following:

Option	Description	Syntax
Token-Ring using MSB	Uses the standard 802.2 IPX header with the noncanonical Token-Ring address bit ordering (MSB).	frame token-ring msb
Token-Ring using LSB	Uses the 802.2 IPX header with the canonical address bit ordering (LSB).	frame token-ring lsb
Token-Ring with 802.2 SNAP using MSB	Uses the 802.2 format with a SNAP header and noncanonical address bit ordering. This encapsulation is used primarily in bridging environments.	frame token-ring_snap msb
Token-Ring with 802.2 SNAP using LSB	Uses the 802.2 format with a SNAP header and canonical address bit ordering.	frame token-ring_snap lsb
Ethernet 2.0	Uses Ethernet version 2.0 protocol 81-37.	frame ethernet_II
Ethernet 802.2	Uses Ethernet 802.3 with 802.2 SA E0.	frame ethernet_8022
Ethernet 802.3	Uses Ethernet 802.3 without any 802.2 header.	frame ethernet_802.3
Ethernet SNAP	Uses 802.3, 802.2 with SNAP PID 00-00-00-81-37.	frame ethernet_SNAP

Syntax:

frame *ipx-encapsulation type*

Note: The frame command cannot be used in the network configuration process to set the IPX encapsulation unless the interface has been configured with IPX.

The IPX encapsulation can also be set in the IPX configuration environment. Refer to the Multiprotocol Switched Services (MSS) Configuring Protocols and Features chapter on Configuring IPX for details.

Example:

```
frame token_ring msb
```

IP-Encapsulation (for Ethernet ATM Forum-Compliant LEC only)

Use the **IP-encapsulation** command to select Ethernet (Ethernet type X'0800') or IEEE 802.3 (Ethernet 802.3 with SNAP). Specify either type **E**thernet or **I**EEE-802.3.

Syntax:

IP-encapsulation	Ethernet
	IEEE-802.3

List

Use the **list** command to list the LE client configuration.

Syntax:

list

LLC

Logical Link Control can be thought of as a “sub-protocol”. It is not accessed directly from either the Talk 6 (configuration) or the Talk 5 (console) environment. Instead, it is accessed from the Token Ring LEC configuration menu by entering an **LLC** command.

Use the **llc** command to access the `LLC Config>` prompt. See“LLC Configuration Commands” on page 336 for more information.

Syntax:

llc

QoS

Use the **qos-configuration** command to get you to the `LEC QoS Config>` prompt from which you can configure Quality of Service as described in “LE Client QoS Configuration Commands” on page 480.

Syntax:

qos-configuration

RIF-Timer (for Token-Ring Forum-compliant LEC only)

Use the **RIF-Timer** command to set the maximum amount of time that information in the RIF is maintained before it is refreshed. Range is 0 to 4096. The default is 120 seconds.

Syntax:

rif-timer *value*

Example:

```
rif-timer 100
```

Set

Use the **set** command to set LE Client parameters.

Syntax:

set

arp-aging-time
arp-cache-size
arp-queue-depth
arp-response-time
auto-config
best-effort-peakrate
bus-connect-retries
conn-completion-time
control-timeout
elan-name
esi-address
flush-timeout
forward-delay
forward-disconnect-timeout
frame-size
initial-control-timeout
lecs-atm-address
les-atm-address
mac-address
multicast-send-avg
multicast-send-peak
multicast-send-type
multiplier-control-timeout
path-switch-delay
reconfig-delay-min
reconfig-delay-max
retry-count
selector
trace
unknown-count
unknown-time
vcc-timeout

arp-aging-time

Sets ARP aging time. This is the maximum time that a LEC will maintain an entry in its LE_ARP cache in the absence of a verification of that relationship. A larger aging time may result in a faster session setup time, but may also use more memory and reacts slower to changes in network configuration.

Valid Values:
An integer number of seconds in the range of 10 to 300.

Default Value:
300

Example:

```
LEC Config> set arp-aging-time 200
```

arp-cache-size
Sets the number of entries in the ARP cache. The size of the ARP cache limits the number of simultaneous data direct VCCs. Larger ARP caches require more memory, but permit the client to simultaneously converse with a larger number of destinations.

Valid Values:
An integer number in the range of 10 to 65535.

Default Value:
5000

Example:

```
LEC Config> set arp-cache-size 10
```

arp-queue-depth
Sets the maximum number of queued frames per ARP cache entry. The LEC enqueues frames when switching the data path from the Multicast Send VCC to a Data Direct VCC. Frames passed to the LEC for transmission will be discarded if the queue is full. A larger queue requires more memory, but results in fewer discarded frames during the data path switch.

Valid Values:
An integer number in the range of 0 to 10.

Default Value:
5

Example:

```
LEC Config> set arp-queue-depth 10
```

arp-response-time
Sets expected ARP response time. This value controls how frequently an unanswered LE ARP request is retried. Larger values result in fewer LE ARPs, which causes less traffic and possibly increase the amount of time before a Data Direct VCC is established.

Valid Values:
An integer number of seconds in the range of 1 to 30.

Default Value:
1 second

Example:

```
LEC Config> set arp-response-time 20
```

auto-config
Specifies whether this LEC uses LECS auto-config mode. Specify YES or NO. The LEC may contact the LECS to obtain the address of its LES and various other configuration parameters. This value must be Yes for the client to use a redundant IBM MSS Server LES.

Valid Values:

If YES, then you do not have to configure the ATM address of the LES.

If NO, then you *must* configure the ATM address of the LES using the **set les-atm-address** command as described on page 324.

Default Value:

NO

Example:

```
LEC Config> set auto-config yes
```

best-effort-peakrate

Sets the Best Effort Peak Rate. Used when establishing best effort multicast send connections.

The maximum peak rate depends on the maximum data rate of the ATM device.

Specify an integer from 1 to the maximum peak rate in Kbps (the definition is the maximum data rate) as follows:

- If ATM maximum data rate is 25 Mbps, the maximum peak rate is 25,000 Kbps.
- If ATM maximum data rate is 155 Mbps, the maximum peak rate is 155,000 Kbps.

Valid Values:

An integer number in the range of 1 - device maximum data rate.

Default Value:

155000

Example:

```
LEC Config> set best-effort-peakrate 24000
```

bus-connect-retries

This parameter sets the maximum number of times that the LEC will attempt to reconnect to the BUS before returning to the initial state.

Valid Values:

0 - 2

Default Value:

1

connection-completion-time

Sets the connection completion time. This is the time interval in which data or a READY_IND message is expected from a calling party.

When a Data Direct VCC is established to the client, the LEC expects data or a READY_IND message within this time period. The LEC will not transmit frames over a Data Direct VCC established to it until receiving data or a READY_IND. This parameter value controls the amount of time which passes before the LEC issues a READY QUERY (in hopes of receiving a READY_IND). Smaller values lead to faster response times, but also to unnecessary transmissions.

Valid Values:

An integer number of seconds in the range of 1 to 10.

Default Value:
4

Example:

```
LEC Config> set connection-completion-time 5
```

control-timeout

This parameter sets the maximum cumulative control timeout of a request.

A current timeout value is initialized to the value of ***initial-control-timeout***. If a response to a request is not received within the current timeout value, the current timeout is multiplied by the value of the ***multiplier-control-timeout*** and the request is reissued. Each time the current timeout value expires, this process is repeated until the current timeout value exceeds the value of ***control-timeout***.

Valid Values:
An integer number of seconds in the range of 10 to 300.

Default Value:
30

Example:

```
LEC Config> set control-timeout 100
```

elan-name

Specifies name of the ELAN that the LEC wishes to join. This is the ELAN name sent to the LECS in the configure request (if the LEC autoconfigures) or to the LES in the join request. The LECS or LES may return a different ELAN name in the response.

Valid Values:
Any character string length of 0 - 32 bytes.

Default Value:
Blank

Note: A blank name (0 length string) is valid.

Example:

```
LEC Config> set elan-name FUZZY
```

esi-address

Sets the ESI portion of the LEC's ATM address.

Specify the ESI portion (octets 13 through 19) of the LEC's ATM address. The ESI and selector combination of the LEC must be unique among all LAN emulation components on the device.

Valid Values:
Any 12 hexadecimal digits.

Default Value:
Burned-in ESI

Example:

```
set esi
Select ESI
   (1) Use burned in ESI
   (2) 11.22.33.44.55.66

Enter selection [1]?
```

flush-timeout

Sets the flush timeout. This is the time limit to wait to receive the LE_FLUSH_RESPONSE after the LE_FLUSH_REQUEST has been sent before taking recovery action. During recovery, any queued frames are dropped and a new flush request is sent.

When switching from the multicast send to a data direct data path, the client sends a flush request over the multicast send VCC. Until a flush response is received, or until the path switch delay expires, frames are queued for the destination.

Valid Values:

An integer number of seconds in the range of 1 to 4.

Default Value:

4

Example:

```
LEC Config> set flush-timeout 3
```

forward-delay

Sets the forward delay. Entries in the LE ARP cache must be periodically re-verified. The forward delay time is the maximum amount of time a remote entry may remain in the cache during a network topology change. Larger aging times may result in stale (invalid) entries, but also cause less re-verification traffic.

Valid Values:

An integer number of seconds in the range of 4 to 30.

Default Value:

15

Example:

```
LEC Config> set forward-delay 10
```

forward-disconnect-timeout

This parameter sets the amount of time that a LEC will wait after losing its last Multicast Forward VCC from the BUS before returning to the initial state. This delay permits the BUS to attempt to reconnect to the client without returning to the initial state.

Valid Values:

10 - 300 seconds

Default Value:

60

frame-size

Sets the frame size.

The value specified for frame-size must be equal to or less than the value specified for ATM max-frame using the ATM INTERFACE> **set max-frame** command as described on page 272.

Valid Values:

1516

4544

9234

18190

Default Value:
If the ELAN type is token ring, the default is 4544. If the ELAN type is Ethernet, the default is 1516.

Example:

```
LEC Config> set frame-size 4544
```

initial-control-timeout
This parameter sets the value of the initial control timeout used in the control timeout algorithm described in 323.

Valid Values:
1 - 10

Default Value:
5

Example:

```
LEC Config> set initial-control-timeout 10
```

lecs-atm-address
Specifies the ATM address of the LECS.

If the client is set to auto configure, it attempts to connect to a LECS. If it is unable to connect to a LECS, then it may try another LECS ATM address. The LECS ATM addresses that are tried, in order, are:

1. This configured LECS address
2. Any LECS address obtained through ILMI
3. The well-known LECS address defined by the ATM Forum.

No default is provided.

Note: This command should be entered on one command line. It is shown here on two lines because of spacing.

Example:

```
LEC Config> set lecs-atm-address
39.84.0F.00.00.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.01
```

les-atm-address
Sets the LES ATM address. This command may be optional or required depending upon the setting of lecs-auto-config as described in the **set auto-config** command on page 321.

- If auto-config is YES, the les-atm-address is not configurable.
- If auto-config is NO, then the les-atm-address is required.

Specify the ATM address of the LES. No default is provided.

Note: This command should be entered on one command line. It is shown here on two lines because of spacing.

Example:

```
LEC Config> set les-atm-address
      39.84.0F.00.00.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.02
```

mac-address
Sets the MAC address for this LE client. You *may* specify that the client use the burned-in MAC address of the ATM interface, or you may specify a

different MAC address. If you have two clients that are bridged together, they should use different MAC addresses.

This MAC address is registered with the LES when the client joins the ELAN.

Valid Values:
Any valid MAC address.

Default Value:
none

Example:

```
LEC Config> set mac-address
  Use adapter address for MAC? [No]
  MAC address []: 10.00.5a.00.00.01
```

multicast-send-avg

Sets the multicast send VCC average rate in Kbps. Used by the LEC for reserving bandwidth on the VCC to the BUS. It specifies the forward and backward sustained cell rate used when setting up a reserved bandwidth multicast send VCC.

This parameter is only applicable when the multicast-send-type is reserved bandwidth. If multicast-send-avg equals multicast-send-peak, then a constant bit rate (CBR) multicast send is signalled. Otherwise, a variable bit rate (VBR) multicast send is signalled. Multicast-send-avg must be less than or equal to multicast-send peak.

A reserved bandwidth multicast send VCC may improve data transfer rates in congested networks, but reserving bandwidth and not using it wastes network resources.

When the multicast-send-type is reserved, then multicast-send-avg and multicast-send-peak must be specified.

Example:

```
LEC Config> set multicast-send-avg 4000
```

multicast-send-peak

Sets the multicast send peak rate in Kbps. Used by LEC for reserving bandwidth on the VCC to the BUS. It specifies the forward and backward peak cell rate used when establishing a reserved bandwidth multicast send VCC.

This parameter is only applicable when the multicast-send-type is reserved bandwidth. If multicast-send-avg equals multicast-send-peak, then a constant bit rate (CBR) multicast send is signalled. Otherwise, a variable bit rate (VBR) multicast send is signalled. Multicast-send-avg must be less than or equal to multicast-send peak.

A reserved bandwidth multicast send VCC may improve data transfer rates in congested networks, but reserving bandwidth and not using it wastes network resources.

When the multicast-send-type is reserved, then multicast-send-avg and multicast-send-peak must be specified.

Example:

```
LEC Config> set multicast-send-peak 155
```

multicast-send-type

Sets the multicast send type. Specifies the method used by the LEC when establishing the multicast send VCC.

If multicast-send-avg equals multicast-send-peak, then a constant bit rate (CBR) multicast send is signalled. Otherwise, a variable bit rate (VBR) multicast send is signalled. Multicast-send-avg must at least equal multicast-send peak.

A reserved bandwidth multicast send VCC may improve data transfer rates in congested networks, but reserving bandwidth and not using it wastes network resources.

When the multicast-send-type is reserved, then multicast-send-no and multicast-send-peak must be specified.

Valid Values:
Best Effort or Reserved

Default Value:
Best Effort

Example:

```
LEC Config> set multicast-send-type best-effort
```

multiplier-control-timeout

This parameter sets the value of the control timeout multiplier used in the control timeout algorithm described on page 323.

Valid Values:
2 - 5

Default Value:
2

Example:

```
LEC Config> set multiplier-control-timeout 5
```

path-switch-delay

Sets the path switch delay.

The LEC must ensure that all frames sent through the BUS to a destination have arrived at the destination before it can start using a Data Direct VCC. This is accomplished using the flush protocol, or by waiting path-switch-delay seconds after sending the last packet to the BUS. Smaller values improve performance, but may result in out-of-order packets in a heavily congested network.

Valid Values:
An integer number of seconds in the range of 1 to 8.

Default Value:
6

Example:

```
LEC Config> set path-switch-delay 5
```

reconfig-delay-min

This parameter sets the minimum delay time when LEC returns to the initial state. This value must be ≤ ***reconfig-delay-max***.

Valid Values:
1 - the value of ***reconfig-delay-max***

Default Value:
1

Example:

```
LEC Config> set reconfig-delay-min  5
```

reconfig-delay-max

This parameter sets the maximum delay time when LEC returns to the initial state. This value must be ≥ ***reconfig-delay-min***.

Valid Values:

1 - 10

Default Value:

5

Example:

```
LEC Config> set reconfig-delay-max 9
```

retry-count

Sets the retry count. This is maximum number of times that the LEC retries an LE_ARP_REQUEST for a specific frame's LAN destination. If no ARP response is received after the specified number of retries, then the entry is purged from the LE ARP cache.

Valid Values:

0, 1, or 2

Default Value:

1

Example:

```
LEC Config> set retry-count 2
```

selector

Specifies the selector portion of the client's ATM address. The combination of ESI and selector must be unique among all LANE components on the device. By default, a unique selector is selected for the configured ESI.

Valid Values:

Any octet, in hexadecimal, that is not in use by another LANE component with the same ESI.

Example:

```
LEC Config> set selector 01
```

trace Enables tracing for the LEC. To perform packet tracing, three steps are required:

1. Enable packet tracing system (under ELS)
2. Enable tracing on the LEC subsystem (under ELS)
3. Enable packet tracing on the desired LECs (using this command).

Valid Values:

Yes or No

Default Value:

No

Example:

```
Token Ring LEC config>set trace
Trace packets on the LEC? [No]?yes
```

unknown-count

Sets the unknown frame count. This is the maximum number of frames for

a specific unicast MAC address or route descriptor that may be sent to the BUS within the time specified by the unknown-time parameter. Larger values decrease the number of discarded frames while increasing the load on the BUS.

Valid Values:
An integer number of frames in the range of 1 to 255.

Default Value:
10

unknown-time
Sets the unknown frame time. This is the time interval during which the maximum number of frames for a specific unicast MAC address or route descriptor (specified by the unknown-count parameter) may be sent to the BUS. Larger values increase the number of discarded frames while decreasing the load on the BUS.

Valid Values:
An integer number of seconds in the range of 1 to 60.

Default Value:
1

Example:

```
LEC Config> set unknown-time 5
```

vcc-timeout
Sets the VCC timeout. Data direct VCCs over which no traffic has been sent for this period of time should be released.

Valid Values: 0 to 31536000 seconds (1 year).

Default Value: 1200

Note: This parameter is meaningful only for SVC connections.

Example:

```
LEC Config> set vcc-timeout 1000
```

Source-Routing (for Token-Ring Forum-Compliant LEC only)

Use the **source-routing** command to enable or disable end station source-routing. Source routing is the process by which end stations determine the source route to use to cross source routing bridges. Source routing allows the IP, IPX, and AppleTalk Phase 2 protocols to reach nodes on the other side of the source route bridge.

This function of the device is not changed whether source routing is enabled or disabled. The default setting is enabled.

Some stations cannot properly receive frames with Source Routing RIF on them. This is especially common among NetWare drivers. Disabling source routing in this situation will allow you to communicate with these stations.

Source routing should be enabled only if there are source-routing bridges on this ring through which you want to bridge IP, IPX, and AppleTalk Phase 2 packets. Source routing must also be enabled so that LLC test response messages can be returned.

Configuring Forum LE Clients

Syntax:

source-routing enable
disable

Example:

```
source-routing disable
```

Configuring an IBM LE Client

This section summarizes and then explains the commands for configuring an IBM LAN Emulation Client.

Enter the appropriate commands at either the `Ethernet-IBM LEC Config>` prompt or the `Token-Ring-IBM LEC Config>` prompt. Commands in the following table apply to both types of LECs except where indicated.

Table 39. IBM LAN Emulation Client Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Frame	Sets the NetWare IPX encapsulation type.
IP-Encapsulation	Sets the IP encapsulation as Ethernet (type X’0800’) or IEEE (802.3 with SNAP). Applies only to Ethernet LECs.
List	Lists the LAN Emulation Client configuration.
LLC	Accesses the `LLC Config>` configuration prompt for Token Ring LECs.
RIF-Timer	Sets the maximum amount of time that information in the RIF is maintained before it is refreshed. Applies only to Token-Ring LECs.
Set	Sets the IBM LAN Emulation Client parameters.
Source-routing	Used to enable or disable source-route bridging. Applies only to Token-Ring LECs.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Frame

Use the **frame** command to set the NetWare IPX encapsulation type. The command options differ depending on the type of LEC (Ethernet or Token-Ring) For Token-Ring LECs, enter one of the following:

Option	Description	Syntax
Token-Ring using MSB	Uses the standard 802.2 IPX header with the noncanonical Token-Ring address bit ordering (MSB).	frame token-ring msb
Token-Ring using LSB	Uses the 802.2 IPX header with the canonical address bit ordering (LSB).	frame token-ring lsb
Token-Ring with 802.2 SNAP using MSB	Uses the 802.2 format with a SNAP header and noncanonical address bit ordering. This encapsulation is used primarily in bridging environments.	frame token-ring_snap msb

Option	Description	Syntax
Token-Ring with 802.2 SNAP using LSB	Uses the 802.2 format with a SNAP header and canonical address bit ordering.	frame token-ring_snap lsb
Ethernet 2.0	Uses Ethernet version 2.0 protocol 81-37.	frame ethernet_II
Ethernet 802.2	Uses Ethernet 802.3 with 802.2 SA E0.	frame ethernet_8022
Ethernet 802.3	Uses Ethernet 802.3 without any 802.2 header.	frame ethernet_802.3
Ethernet SNAP	Uses 802.3, 802.2 with SNAP PID 00-00-00-81-37.	frame ethernet_SNAP

Syntax:

frame *ipx-encapsulation-type*

Note: The frame command cannot be used in the network configuration process to set the IPX encapsulation unless the interface has been configured with IPX.

The IPX encapsulation can also be set in the IPX configuration environment. Refer to the Multiprotocol Switched Services (MSS) Configuring Protocols and Features chapter on Configuring IPX for details.

Example: `frame token_ring msb`

IP-Encapsulation (for Ethernet-IBM LEC only)

Use the **IP-encapsulation** command to select Ethernet (Ethernet type X'0800') or IEEE 802.3 (Ethernet 802.3 with SNAP). Specify either type **E**thernet or **I**EEE-803.3.

Syntax:

IP-encapsulation *type*

Example: `IP-encapsulation E`

List

Use the **list** command to list the LE client configuration.

Syntax: list

LLC

Logical Link Control can be thought of as a "sub-protocol". It is not accessed directly from either the Talk 6 (configuration) or the Talk 5 (console) environment. Instead, it is accessed from the Token Ring LEC configuration menu by entering an **LLC** command.

Use the **llc** command to access the `LLC Config>` prompt. See"LLC Configuration Commands" on page 336 for more information.

Syntax:

llc

RIF-Timer (for Token-Ring-IBM LEC only)

Use the **RIF-Timer** command to set the maximum amount of time that information in the RIF is maintained before it is refreshed. Range is 0 to 4096. The default is 120.

Syntax:

rif-timer

Example: `rif-timer 100`

Set

Use the **set** command to set IBM LE Client parameters.

Syntax: set

- backward-peakrate
- esi-address
- frame-size
- forward-peakrate
- keep-alive-count
- les-atm-address
- mac-address
- mac-cache-size
- mac-cache-aging-period
- rd-cache-size
- rd-cache-aging-period
- registration interval
- retry-count
- selector
- trace

backward-peakrate

This parameter specifies the maximum data rate (backward peak rate), in Kbps, of the ATM device for all LAN emulation connections.

Specify an integer from 1 to the maximum data rate of the ATM device.

Default: line rate in Kbps

Example:

```
LEC Config> set backward-peakrate 155000
```

esi-address

Sets the ESI portion of the client's ATM address.

Valid Values:

Any 12 hexadecimal digits.

Default Value:

Burned-in ESI

Example:

```
token ring lec config>set esi
Select ESI
   (1) Use burned in ESI
   (2) 11.22.33.44.55.66

Enter selection [1]?
```

frame-size

Sets the frame size.

The value specified for frame-size must be equal to or less than the value specified for ATM max-frame using the ATM INTERFACE> **set max-frame** command as described on page 272. The specified maximum frame size includes any Layer 2 header information. All transparently bridged LANs must have the same maximum frame size.

Valid Values:

1024 - 17843

Default Value:

If the ELAN type is token ring, the default is 4551. If the ELAN type is Ethernet, the default is 1523.

forward-peakrate

This parameter specifies the maximum data rate (forward peak rate), in Kbps, of the ATM device for all LAN emulation connections.

Specify a decimal integer between 1 and the maximum data rate of the ATM device.

Default: data rate in Kbps

Example:

```
Ethernet IBM LEC Config> set forward-peakrate 155000
```

keep-alive-count

Specifies the number of times that the LEC sends a registration message without requiring a response from the LES.

Valid Values: 5 to 50

Default Value: 10

Example:

```
Ethernet IBM LEC Config> set keep-alive-count 20
```

les-atm-address

Sets the LES ATM address.

Specify the ATM address of the LES. *

Note: This command should be entered on one command line. It is shown here on two lines because of spacing.

Example:

```
Ethernet IBM LEC Config> set les-atm-address
      39.84.0F.00.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.02
```

mac-address

Sets the MAC address for this LE client. You *may* specify that the client use the burned in MAC address, of the ATM interface, or you may specify a different MAC address. If you have two clients that are bridged together, they should use different MAC addresses.

Valid Values:

Any valid MAC address.

Default Value:
none

Example:

```
Ethernet IBM LEC Config> set mac-address
  Use adapter address for MAC? [No]
  MAC address []: 10.00.5a.00.00.01
```

mac-cache-size
Specifies the maximum number of MAC entries that the LEC caches.

Valid Values: 5 to 1024.

Default Value: 32

Example:

```
Ethernet IBM LEC Config> set mac-cache-size 48
```

mac-cache-aging-period
Specifies the amount of time (in seconds) after which MAC addresses are aged out of the cache, if not refreshed.

Valid Values: 1 to 300

Default Value: 60

Example:

```
Ethernet IBM LEC Config> set mac-cache-aging-period 120
```

rd-cache-size
Specifies the maximum number of route descriptor entries that the LEC caches.

Valid Values: 5 to 1024

Default Value: 32

Example:

```
Ethernet IBM LEC Config> set rd-cache-size 48
```

rd-cache-aging-count
Specifies the amount of time (in seconds) after which entries are aged out of the route descriptor cache, if not refreshed.

Valid Values: 1 to 300

Default Value: 60

Example:

```
Ethernet IBM LEC Config> set rd-cache-aging-period 120
```

registration-interval
Specifies the frequency (in seconds) that the LEC sends registration messages to the LES.

Valid Values: 30 to 240

Default Value: 60

Example:

```
Ethernet IBM LEC Config> set registration-interval 75
```

retry-count
Sets the retry count. This is maximum number of times that the LEC retries an LE_ARP_REQUEST for a specific frame's LAN destination.

Valid Values:
An integer number in the range of 2 to 10.

Default Value:
3

Example:

```
Ethernet IBM LEC Config> set retry-count 2
```

selector
Specifies the selector portion of the client's ATM address. The combination of ESI and selector must be unique among all LANE components on the device. By default, a unique selector is selected for the configured ESI.

Valid Values:
Any octet, in hexadecimal, that is not in use by another LANE component with the same ESI.

Example:

```
LEC Config> set selector 01
```

trace Sets packet trace for the LEC.

Valid Values:
Yes or No

Default Value:
No

To perform packet tracing, three steps are required:

1. Enable packet tracing system (under ELS)
2. Enable tracing on the LEC subsystem (under ELS)
3. Enable packet tracing on the desired LECs (using this command).

Example:

```
Token Ring LEC config>set trace
Trace packets on the LEC? [No]?yes
```

Source-routing (for Token-Ring-IBM LEC only)

Use the **source-routing** command to enable or disable end station source-routing. Source routing is the process by which end stations determine the source route to use to cross source routing bridges. Source routing allows the IP, IPX, and AppleTalk Phase 2 protocols to reach nodes on the other side of the source route bridge.

This function of the device is not changed whether source routing is enabled or disabled. The default setting is enabled.

Some stations cannot properly receive frames with Source Routing RIF on them. This is especially common among NetWare drivers. Disabling source routing in this situation will allow you to communicate with these stations.

Source routing should be enabled only if there are source-routing bridges on this ring through which you want to bridge IP, IPX, and AppleTalk Phase 2 packets. Source routing must also be enabled so that LLC test response messages can be returned.

Configuring IBM LE Clients

Syntax:

source-routing	enable
	disable

Example: `source-routing disable`

LLC Configuration Commands

This section summarizes and then explains all of the LLC commands. These commands, shown in Table 40, let you monitor the LLC while passing packets over an SNA network.

Table 40. LLC Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
List	Displays configuration information.
Set	Allows the user to dynamically configure LLC parameters that are valid for the life of the session.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to display configuration information.

Syntax:

list

Set

Use the **set** command to dynamically configure the LLC parameters on a current LLC session. Any changes that you make to the parameters are effective for the life of session.

Attention: Changing LLC parameters from the default can affect how the LLC protocol works.

Syntax:

set	n2-max_retry *count*
	n3-frames-rcvd-before-ack *count*
	nw-acks-to-inc-ww *count*
	rw-receive-window *seconds*
	t1-reply-timer *seconds*
	t2-receive-ack-timer *seconds*
	ti-inactivity-timer *seconds*
	tw-transmit-window *seconds*

n2-max_retry
The maximum number of retries by LLC protocol. For example, N2 is the maximum number of times the LLC transmits an RR without receiving an acknowledgment when the inactivity timer expires. Default is 8. Minimum is 1. Maximum is 127.

n3-frames-rcvd-before-ack
This value is used with the T2 timer to reduce acknowledgment traffic for received I-frames. Set this counter to a specified value. Each time an I-frame is received, this value is decremented. When this counter reaches 0 or the T2 timer expires, an acknowledgment is sent. Default is 1. Minimum is 1. Maximum is 255.

nw-acks-to-inc-ww
This field is set to a default value of 1.

rw-receive-window
Sets the number of I-frames that can be recived before an RR is transmitted. Default is 2. Minimum is 1. Maximum is 127.

t1-reply-timer
This timer expires when the LLC fails to receive a required acknowledgment or response from the other LLC station. When this timer expires, an RR is sent with the poll bit set and T1 is started again. If the LLC receives no response after the configured maximum number of retries (N2), the link underneath is declared inoperative. Default is 1. Minimum is 1. Maximum is 256.

t2-receive-ack-timer
This timer is used to delay sending of an acknowledgment for a received I-format frame. This timer is started when an I-frame is received and reset when an acknowledgment is sent. If this timer expires, LLC2 sends an acknowledgment as soon as possible. Set this value so that it is less than that of T1. This insures that the remote LLC2 peer receives the delayed acknowledgment before the T1 timer expires. Default is 1 (100 ms). Minimum is 1. Maximum is 2560.

Note: If this timer is set to 1 (the default) it will not run (for example, **n3-frames-rcvd-before-ack=1**).

ti-inactivity-timer
This timer expires when the LLC does not receive a frame for a specified time period. When this timer expires the LLC transmits an RR until the other LLC responds or the N2 timer expires. Default is 30 seconds. Minimum is 1 second. Maximum is 256 seconds.

tw-transmit-window
Sets the maximum number of I-frames that can be sent before receiving an RR. Assuming that the other end of the LLC session can actually receive this many consecutive I-frames, and the router has enough heap memory to keep copies of these frames until an acknowledgment is received, increasing this value may increase the throughput. Default is 2. Minimum is 1. Maximum is 127.

Accessing the LEC Monitoring Environment

Use the following procedure to access the LEC monitoring commands. This process gives you access to the LEC *monitoring* process.

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, refer to “What is the OPCON Process?” on page 75.) For example:

```
* talk 5
+
```

   After you enter the **talk 5** command, the GWCON prompt (+) displays on the console. If the prompt does not appear when you first enter configuration, press **Return** again.

2. At the + prompt, enter the **network ?** command to display the network interface numbers for which the router is currently configured, and enter the *interface number* for the LEC you wish to monitor. For example:

```
+ network ?

1  : ATM Ethernet LAN Emulation: ETH
2  : IP Protocol Network
3  : Bridge Application
5  : CHARM ATM Adapter
Network number [0]? 1
LEC+
```

   The LEC monitoring prompt (LEC+), is displayed.

   If you know the interface number of the LEC you wish to monitor, enter the **network** command followed by the *interface number* of the LEC.

```
+ network 1
LEC+
```

LEC Monitoring Commands

This section summarizes and then explains the LEC monitoring commands. You can access LEC monitoring commands at the LEC+ prompt. Table 41 shows the commands.

Table 41. LE Client Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
List	Lists: • LEC Address Resolution Table (ARP) • LEC configuration • Data Direct VCC information • Group addresses • RIF information • LEC statistics • VCC table.
LLC	Gets you to the LLC> monitoring prompt for Token Ring LECs.
MIB	Displays LEC MIB objects including: • LEC MIB Configuration Table • LEC MAC ARP Table • LEC Route Descriptor Table • LEC MIB Server VCC Tables • LEC MIB Statistics Table • LEC MIB Status Table

Table 41. LE Client Monitoring Command Summary (continued)

Command	Function
QoS	Gets you to the LEC x QoS+ prompt from which you can monitor Quality of Service as described in “Quality of Service Monitoring Commands” on page 487.
Trace	Sets packet tracing on or off or sets a trace address or trace mask.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to list the LEC Address Resolution Table (ART), list the LEC configuration, list Data Direct VCC information, or list LEC statistics.

Syntax:

list arp-table
configuration
data-direct-vccs
group
rif
statistics
vcc-table

arp Lists the LEC Address Resolution Table (entries in the ARP cache).

Example:

```
LEC+ list arp

         LEC Address Resolution (LE ARP Cache) Table

  Max Table Size          = 10
  Free Table Entries      = 10
  Current Mac Entries     = 0
  Current RD Entries      = 0
  Arp Aging Time          = 300
  Verify Sweep Interval   = 60

                                Xmit  BUS   Arp
                          Conn  Queue Frame Retry Aging
 MAC Address     Remote Handle Depth Count Count Timer  Destination ATM Ad
                                                                    dress
 ------------------------------------------------------------------------
 40.00.00.00.00.09 False 652   0     0     0     60     39.99.99.99.99.99.
                               99.00.00.99.99.30.02.40.00.00.00.00.09.81
```

Note: The Sweep Interval is always one-fifth of the ARP Aging Timer value.

Max Table Size
The total number of entries available

Free Table Entries
The number of free entries

Current MAC Entries

Current RD Entries
Route Descriptor ATM entries

ARP Aging Time
Time for an entry to be aged out

Verify Sweep Interval

MAC Address

Remote

Connection Handle

Queue Depth

Xmit Frame Count

BUS Retry Count

ARP Aging Timer

Destination ATM Address

configuration

Lists the LEC configuration.

For Ethernet:

Example:

```
IBM LEC+ list config
                    ATM IBM LEC Configuration
   Physical ATM interface number             = 0
   LEC interface number              = 7
   Primary ATM address
          ESI address                = Use burned in addr
          Selector byte              = 0x3
   Emulated LAN type                 = Ethernet IBM
   Maximum frame size                = 1523
   LE Client MAC address             = Use burned in addr
   LE Server ATM address             = 00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00
   Forward Peak Rate                 = 155000
   Backward Peak Rate                = 155000
    MAC cache size                    = 32
   MAC cache aging period            = 60
   Route Descriptor cache size       = 32
   Route Descriptor aging period     = 60
   LES Registration interval         = 60
   LES Registration retry count      = 3
   LES keep alive count              = 10
   Packet trace                      = No
   IP Encapsulation                  = ETHER
```

For Token Ring IBM:

Example:

```
IBM LEC+list config

                      ATM IBM LEC Configuration
   Physical ATM interface number             = 0
   LEC interface number              = 10
   Primary ATM address
          ESI address                = Use burned in addr
          Selector byte              = 0x6
   Emulated LAN type                 = Token Ring IBM
   Maximum frame size                = 4551
   LE Client MAC address             = Use burned in addr
   LE Server ATM address             = 39.84.07.00.00.00.00.00.00.00.00.00.01.10.00.5A.DD.DA.02
   Forward Peak Rate                 = 155000
   Backward Peak Rate                = 155000
    MAC cache size                    = 32
```

```
   MAC cache aging period           = 60
   Route Descriptor cache size      = 32
   Route Descriptor aging period    = 60
   LES Registration interval        = 60
   LES Registration retry count     = 3
   LES keep alive count             = 10
   Packet trace                     = No
   RIF Aging Timer                  = 120
   Source Routing                   = Enabled
```

For Token Ring Forum Compliant:

Example:

```
LEC+ list config

   Physical ATM interface number = 0
   LEC interface number          = 9
   LEC ATM address               = 39.99.99.99.99.99.99.00.00.99.99.31.01.09.FC.DD.D0.32.70.0A
   LEC MAC address               = 40.00.82.10.17.09
   lecConfigMode                 = Manual
   lecConfigLanType              = 802.5 - Token Ring
   lecConfigMaxDataFrameSize     = 4544
   lecConfigLanName              =
   lecConfigLesAtmAddress        = 39.99.99.99.99.99.99.00.00.99.99.31.01.40.00.82.10.17.00.09
   lecControlTimeout             = 30
   lecMaxUnknownFrameCount       = 10
   lecMaxUnknownFrameTime        = 1
   lecVccTimeoutPeriod           = 1200
   lecMaxRetryCount              = 1
   lecAgingTime                  = 300
   lecForwardDelayTime           = 15
   lecExpectedArpResponseTime    = 1
   lecFlushTimeout               = 4
   lecPathSwitchingDelay         = 6
   lecLocalSegmentId             = 0x0
   lecMulticastSendType          = 1
   lecMulticastSendAvgRate       = 365566
   lecMulticastSendPeakRate      = 365566
   lecConnectionCompleteTimer    = 4
   lecInitialControlTimeout      = 5
   lecControlTimeoutMultiplier   = 2
   V2 Capable                    = TRUE
   lecForwardDisconnectTimeout   = 60
   lecMinReconfigDelay           = 1
   lecMaxReconfigDelay           = 5
   lecMaxBusConnectRetries       = 0
   lecElanId                     = 0
   ExplorerExclude               = TRUE
   LE ARP queue depth            = 5
   LE ARP cache size             = 5000
   Forward peakrate              = 365566
   Backward peakrate             = 365566
   Packet trace                  = Off
   RIF aging timer               = 120
   Source Routing                = enabled
```

See “Set” on page 319 for a definition of the parameters shown in the above examples.

data Lists the LEC Data Direct VCC information.

Example:

```
LEC+ list data

          LEC Data Direct VCC Table

   Max Table Size     = 1019    Max no of SVC connections
   Current Size       = 0       Currently used
   Inactivity Timeout = 1200    No Data Xfer Timeout before connection is
                                closed (seconds)
   Sweep Interval     = 60
      Conn              Inactive  User
      Handle  VPI  VCI   Timer    Count  Destination ATM Address
    ------------------------------------------------------------------------------

       652     0  7241    300       1    39.99.99.99.99.99.99.00.00.99.99.30.02.
                                         40.00.00.00.00.09.81


    ------------------------------------------------------------------------------
```

group Lists the group addresses in use by the LEC.

rif Lists the MAC address to Routing Information Field (RIF) mappings in use by the LEC.

statistics
Lists LEC statistics.

Example:

```
LEC+ list stat

          LEC Statistics

   In Octets.high     = 0       No of Bytes received
   In Octets.low      = 346
   In Discards        = 2       Packets discarded
   In Errors          = 0       Rx.Errors
   In Unknown Protos  = 0       Unknown protocols received
   Out Octets.high    = 0       No of Bytes xmitted.
   Out Octets.low     = 0
   Out Discards       = 0
   Out Errors         = 0       Tx.Errors
   In Frames          = 0
   Out Frames         = 0
   In Bytes           = 0
   Out Bytes          = 0
```

VCC table
Lists VCC table.

Example:

```
LEC+ list vcc
```

LLC

Logical Link Control can be thought of as a "sub-protocol". It is not accessed directly from either the Talk 6 (configuration) or the Talk 5 (console) environment. Instead, it is accessed from the Token Ring LEC monitoring menu by entering an **LLC** command.

Use the **llc** command to access the LLC> prompt. See"LLC Monitoring Commands" on page 347 for more information.

Syntax:

llc

MIB

Use the **mib** command to display MIB objects.

Note: Some of this information may be displayed in a different format using the **list** command.

Syntax:

mib config-table
mac-arp-table
rd-arp-table
server-vcc-table
statistics-table

status-table

super-elan-table

config Displays the LEC MIB Configuration Table.

Example:

```
LEC+ mib config

 lecConfigTable:
 lecConfigMode                 = Manual
 lecConfigLanType              = 802.3 - Ethernet
 lecConfigMaxDataFrameSize     = 1516
 lecConfigLanName              =
 lecConfigLesAtmAddress        = 39.84.0F.00.00.00.00.00.11.23.24.24.24.24.55.66.77.88.99.00
 lecControlTimeout             = 120
 lecMaxUnknownFrameCount       = 1
 lecMaxUnknownFrameTime        = 0
 lecVccTimeoutPeriod           = 1200
 lecMaxRetryCount              = 1
 lecAgingTime                  = 300
 lecForwardDelayTime           = 15
 lecExpectedArpResponseTime    = 1
 lecFlushTimeout               = 4
 lecPathSwitchingDelay         = 6
 lecLocalSegmentId             = 0
 lecMulticastSendType          = 1


 lecMulticastSendAvgRate       = 155000000
 lecMulticastSendPeakRate      = 155000000
 lecConnectionCompleteTimer    = 4
```

lecConfigMode
LEC config mode: AUTO or MANUAL. If AUTO, LEC Uses LECS to get the LES ATM address.

lecConfigLanType
LAN type, either Ethernet or token-ring

lecConfigMaxDataFrameSize
Maximum frame size

lecConfigLanName
ELAN Name

lecConfigLesAtmAddress
LE Server ATM address

lecControlTimeout
Timeout for request/response control frame

lecMaxUnknownFrameCount
Maximum number of unknown frames

lecMaxUnknownFrameTime
Period in which LEC will send a maximum of MaxUnknownFrameCount frames to the BUS for a given unicast LAN Destination, and it must also initiate the address resolution protocol to resolve that LAN Destination.

lecVccTimeoutPeriod
Inactivity timeout of SVC Data Direct VCCs

lecMaxRetryCount
LE ARP retry count

lecAgingTime
Life of unverified entry in the ARP table

lecForwardDelayTime

lecExpectedArpResponseTime
ARP Request/Response cycle time

lecFlushTimeout
LE Flush Request/Flush Reply timeout period

lecPathSwitchingDelay

lecLocalSegmentId
Segment ID of emulated LAN. Only for 802.5 clients

lecMulticastSendType
Signaling parameter used by LEC for multicast send VCC

lecMulticastSendAvgRate
Signaling parameter used by LEC for multicast send VCC

lecMulticastSendPeakRate
Signaling parameter used by LEC for multicast send VCC

lecConnectionCompleteTimer

mac Displays the LEC MAC ARP Table

rd Displays the LEC Route Descriptor Table

server Displays the LEC MIB Server VCC Tables

Example:

```
LEC+ mib server

lecServerVccTable:
   lecConfigDirectInterface      = 0
   lecConfigDirectVpi            = 0
   lecConfigDirectVci            = 0
   lecControlDirectInterface     = 1
   lecControlDirectVpi           = 0
   lecControlDirectVci           = 38
   lecControlDistributeInterface = 1
   lecControlDistributeVpi       = 0
   lecControlDistributeVci       = 37
   lecMulticastSendInterface     = 1
   lecMulticastSendVpi           = 0
   lecMulticastSendVci           = 34
   lecMulticastForwardInterface  = 1
   lecMulticastForwardVpi        = 0
   lecMulticastForwardVci        = 33
```

lecConfigDirectInterface
The interface associated with the Configuration Direct VCC

lecConfigDirectVpi
VPI which identifies the above VCC if it exists

lecConfigDirectVci
VCI which identifies the above VCC if it exists

lecControlDirectInterface
The interface associated with the Control Direct VCC

lecControlDirectVpi
VPI which identifies the above VCC if it exists

lecControlDirectVci
VCI which identifies the above VCC if it exists

lecControlDistributeInterface
The interface associated with the Control Distribute VCC

lecControlDistributeVpi
VPI which identifies the above VCC if it exists

lecControlDistributeVci
VCI which identifies the above VCC if it exists

lecMulticastSendInterface
The interface associated with the Multicast Send VCC

lecMulticastSendVpi
VPI which identifies the above VCC if it exists

lecMulticastSendVci
VCI which identifies the above VCC if it exists

lecMulticastForwardInterface
The interface associated with the Multicast Forward VCC

lecMulticastForwardVpi
VPI which identifies the above VCC if it exists

lecMulticastForwardVci
VCI which identifies the above VCC if it exists

statistics
Displays the LEC MIB Statistics Table.

Example:

```
LEC+ mib statistics

lecStatisticsTable:
   lecArpRequestsOut             = 1
   lecArpRequestsIn              = 0
   lecArpRepliesOut              = 0
   lecArpRepliesIn               = 1
   lecControlFramesOut           = 2
   lecControlFramesIn            = 2
   lecSvcFailures                = 1
```

lecArpRequestsOut
No. of LE ARP requests sent by this LEC

lecArpRequestsIn
No. of LE ARP requests received by this LEC

lecArpRepliesOut
No. of LE ARP responses sent by this LEC

lecArpRepliesIn
No. of LE ARP responses received by this LEC

lecControlFramesOut
No. of Control Packets sent by this LEC

lecControlFramesIn
No. of Control Packets received by this LEC

lecSvcFailures
The total number of:

- Outgoing LAN Emulation SVCs which this client tried but failed, to open
- Incoming LAN Emulation SVCs which this client tried, but failed to establish
- Incoming LAN Emulation SVCs which this client rejected for protocol or security reasons

status Lists MIB status.

Example:

```
LEC+ mib status

lecStatusTable:
   lecPrimaryAtmAddress          = 39.84.0F.00.00.00
   Client ATM address=           = 00.00.00.00.00.01.10.00.5A.00.DE.AD.03
   lecId                         = 1                  Assigned by LES
   lecInterfaceState             = Operational        State of the LEC
   lecLastFailureRespCode        = None               Error code from last
                                                      failed Config/Join resp.
   lecLastFailureState           = Initial State      State of LEC when
                                                      updating above field.
   lecProtocol                   = 1                  Protocol specified by
                                                      LEC in Join requests.
   LecVersion                    = 1                  LEC Protocol Version
                                                      of above
   lecTopologyChange             = False
   lecConfigServerAtmAddress     = 00.00.00.00.00.00.
   ATM Address of LECS           = 00.00.00.00.00.00.00.00.00.00.00.00.00.00
   lecConfigSource               = Did not use LECS
   lecActualLanType              = 802.3 - Ethernet   Frame format currently
                                                      used by LEC
   lecActualMaxDataFrameSize     = 1516
   lecActualLanName              = ETH                Name of emulated LAN
                                                      that LEC joined.
   lecActualLesAtmAddress        = 39.84.0F.00.00.00.
   ATM Address of LES            = 00.00.00.00.00.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.02
   lecProxyClient                = False              Is LES acting like a
                                                      proxy ?
```

super-elan

Example:

```
LEC+ mib super-elan
```

QoS Information

Use the **qos-information** command to get to the `LEC x QoS+` prompt from which you can monitor Quality of Service as described in “Quality of Service Monitoring Commands” on page 487.

Syntax:

qos-information

Trace

Use the **trace** command to turn packet tracing on or off on the LEC. See “Packet-trace Monitoring Commands” on page 204 for more information.

Use the **trace mac-address** command to limit the data traced. A packet will only be traced if its destination or source MAC address logically ANDed with the trace MAC mask equals the trace MAC address logically ANDed with the trace MAC mask.

Syntax:

trace

LLC Monitoring Commands

This section summarizes and then explains all of the LLC commands. These commands, shown in Table 42, let you monitor the LLC while passing packets over an SNA network.

Table 42. LLC Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
List	Displays configuration information.
Set	Allows the user to dynamically configure LLC parameters that are valid for the life of the session.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to display configuration information.

Syntax:

list

Set

Use the **set** command to dynamically configure the LLC parameters on a current LLC session. Any changes that you make to the parameters are effective for the life of session.

Attention: Changing LLC parameters from the default can affect how the LLC protocol works.

Syntax:

set n2-max_retry *count*
n3-frames-rcvd-before-ack *count*
nw-acks-to-inc-ww *count*
t1-reply-timer *seconds*
t2-receive-ack-timer *seconds*
ti-inactivity-timer *seconds*
tw-transmit-window *seconds*

n2-max_retry
The maximum number of retries by LLC protocol. For example, N2 is the maximum number of times the LLC transmits an RR without receiving an acknowledgment when the inactivity timer expires. Default is 8. Minimum is 1. Maximum is 127.

n3-frames-rcvd-before-ack
This value is used with the T2 timer to reduce acknowledgment traffic for received I-frames. Set this counter to a specified value. Each time an

I-frame is received, this value is decremented. When this counter reaches 0 or the T2 timer expires, an acknowledgment is sent. Default is 1. Minimum is 1. Maximum is 255.

nw-acks-to-inc-ww
This field is set to a default value of 1.

t1-reply-timer
This timer expires when the LLC fails to receive a required acknowledgment or response from the other LLC station. When this timer expires, an RR is sent with the poll bit set and T1 is started again. If the LLC receives no response after the configured maximum number of retries (N2), the link underneath is declared inoperative. Default is 1. Minimum is 1. Maximum is 256.

t2-receive-ack-timer
This timer is used to delay sending of an acknowledgment for a received I-format frame. This timer is started when an I-frame is received and reset when an acknowledgment is sent. If this timer expires, LLC2 sends an acknowledgment as soon as possible. Set this value so that it is less than that of T1. This insures that the remote LLC2 peer receives the delayed acknowledgment before the T1 timer expires. Default is 1 (100 ms). Minimum is 1. Maximum is 2560.

Note: If this timer is set to 1 (the default) it will not run (for example, **n3-frames-rcvd-before-ack=1**).

ti-inactivity-timer
This timer expires when the LLC does not receive a frame for a specified time period. When this timer expires the LLC transmits an RR until the other LLC responds or the N2 timer expires. Default is 30 seconds. Minimum is 1 second. Maximum is 256 seconds.

tw-transmit-window
Sets the maximum number of I-frames that can be sent before receiving an RR. Assuming that the other end of the LLC session can actually receive this many consecutive I-frames, and the router has enough heap memory to keep copies of these frames until an acknowledgment is received, increasing this value may increase the throughput. Default is 2. Minimum is 1. Maximum is 127.

Chapter 24. Using LAN Emulation Services

This chapter describes how to use LAN Emulation Services for an Emulated LAN (ELAN).

About LAN Emulation Services

LAN Emulation (LE) protocols allow ATM networks to appear as local area networks such as Ethernet or Token-Ring. An emulated LAN (ELAN) provides flexibility in handling moves, adds, and changes to your network topology. A client's association with an ELAN is logical and is independent of physical location. Consequently, re-configuration is not required when a station is physically moved, provided the station's ELAN *membership* is retained. A station can be a member of multiple ELANs. Wiring modifications are not required when a station is moved from one ELAN to another.

An ELAN is a collection of LAN Emulation Clients (LECs) that are coordinated by LAN Emulation (LE) Services. There are three standard LE Services components that provide services for your ELANs:

- LE Server (LES)
- Broadcast and Unknown Server (BUS)
- LE Configuration Server (LECS)

This chapter describes configuration of the LES, BUS, and LECS components. For a description of LAN Emulation Client (LEC, not to be confused with LECS), refer to "Chapter 22. Using LAN Emulation Clients" on page 311.

The MSS Server has an additional LE Services component that provides a value-added security feature to LE Services. For additional detail on this security feature and on the overall LAN Emulation environment, refer to the *Multiprotocol Switched Services (MSS) Configuration and Operations Guide*.

© Copyright IBM Corp. 1996, 1998

Chapter 25. Configuring and Monitoring LAN Emulation Services

This chapter describes how to configure and control operational LE services. "Chapter 24. Using LAN Emulation Services" on page 349 described the use of LE services. These commands can be used to modify the static memory of the router, and the changes would not take effect until the router is restarted.

There are many components to the LE Services monitoring environment. There is a component for the LECS, for the LES-LECS Security interface, and for each individual LES-BUS.

From the top-level LE Services console, you can enter into a monitoring environment for any particular component, or you can create a new LES-BUS component.

This chapter includes the following sections:

- "Accessing the LAN Emulation Services Environment"
- "Configuration Commands for a LES-BUS" on page 354
- "Configuration Commands for a LECS" on page 374
- "Configuration Commands for the Access Control of a LECS" on page 380
- "Configuration Commands for ELANs at the LECS" on page 382
- "Configuration Commands for ELAN Detailed Configuration" on page 384
- "Configuration Commands for the Policies of a LECS" on page 396
- "Configuration Commands for Security for ELANs" on page 398
- "Accessing the LAN Emulation Services Monitoring Environment" on page 400
- "Monitoring Commands for LAN Emulation Services" on page 400
- "Monitoring Commands for LES-BUS" on page 404, which includes the Broadcast Manager Console
- "Monitoring Commands for LECS" on page 442
- "Monitoring Commands for the Access Control of a LECS" on page 453
- "Monitoring Commands for ELANs at the LECS" on page 454
- "Monitoring Commands for ELAN Details at the LECS" on page 457
- "Monitoring Commands for LECS Policies" on page 466
- "Monitoring Commands for Security for LE Service" on page 469, the LES-LECS interface to validate joins

Individual LE Service components can be stopped, modified, or restarted without restarting the entire router.

Accessing the LAN Emulation Services Environment

To get to the LE-services environment, enter the **le-services** command at the `ATM config>` prompt:

© Copyright IBM Corp. 1996, 1998

Accessing LAN Emulation Services

```
ATM config> le-services
LAN Emulation Services user configuration
LE Services config>
```

To start the configuration process, enter the following commands at the `LE Services config>` prompt:

Table 43. LAN EMULATION Services Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Lecs	Enters the LECS Configuration environment. For additional information, see “Configuration Commands for a LECS” on page 374.
Les-bus	Enters the LES-BUS Configuration environment for a particular ELAN. For additional information, see “Configuration Commands for a LES-BUS” on page 354.
List	Lists all LES-BUSs that you have configured.
Rename	Changes the name of the LES-BUS.
Security	Enters the LES-LECS Security Interface Configuration environment. For additional information, see “Configuration Commands for Security for ELANs” on page 398.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Note: For a description of addressing requirements in this environment, see “How to Enter Addresses” on page 255.

Lecs

Type the **lecs** command at the `LE Services config>` prompt to enter the LECS Configuration environment. The LECS Configuration environment is characterized by the `LECS config>` prompt.

Syntax:

lecs

Example:

```
LE Services config> lecs
LAN Emulation Configuration Server configuration
LECS config>
```

For additional information, see “Configuration Commands for a LECS” on page 374.

Les-bus

Type the **les-bus** command at the `LE Services config>` prompt to enter the LES-BUS Configuration environment for a particular LES-BUS. A selection list will appear, or you can use the **list** command to display all of the currently configured LES-BUSs. The LES-BUS Configuration environment is characterized by the `LES-BUS Config for ELAN 'n'>` prompt.

Syntax:

les-bus elan-name

item-number

elan-name

Name of the ELAN

item-number
Item number from selection list

Example: les-bus

```
LE Services config>les-bus
  (  1) <<< New LES/BUS >>>
  (  2) Test Ethernet Elan
  (  3) Test Token Ring Elan
Choice of LES/BUS [1]? 3
LES-BUS configuration
LES-BUS config for ELAN 'Test Token Ring Elan'>
```

Example: les-bus *elan-name*

```
LE Services config>les-bus Test Token Ring Elan
LES-BUS configuration
LES-BUS config for ELAN 'Test Token Ring Elan'>
```

Example: les-bus *item-number*

```
LE Services config>les-bus 3
LES-BUS configuration
LES-BUS config for ELAN 'Test Token Ring Elan'>
```

For additional information, see “Configuration Commands for a LES-BUS” on page 354.

List

Enter the **list** command to display a list of all the ELANs that are served by LES-BUSs configured on the MSS Server.

Syntax:

list

Example:

```
LE Services config> list
List of Configured LES-BUS(s)

ELAN Type  (E=Ethernet/802.3, T=Token Ring/802.5)
| Interface #
| | Enabled                                                Max.
| | |                                                      Frame   Redundancy
| | | ELAN Name                       LES ESI       Sel    Size    Role
- - - ------------------------------- ------------  ---    -----   ----------
E 0 Y Test Ethernet Elan              400082104001  x02     4544   (disabled)
T 0 Y Test Token Ring Elan            400082104001  x03     4544   (disabled)
```

Rename

Enter the **rename** command to change the name of a LES-BUS.

Note: If you rename a LES-BUS, simply restarting the LES-BUS from the LES-BUS Console will not reflect the newly configured name. To rename an operational LES-BUS, you must either reload, or use the LES-BUS Console command **delete**, then the LAN Emulation Services Console command **create**.

Syntax:

rename

Example:

```
LE Services config> rename
Existing ELAN Name []? test
New ELAN Name []? newtest
```

Security

Type the **security** command to enter the LES-LECS Security Interface Configuration environment. This environment is characterized by the `LECS INTERFACE config>` prompt.

Syntax:

security

Example:

```
LE Service config> security
LECS Interface configuration
LECS INTERFACE config>
```

For additional information, see “Configuration Commands for Security for ELANs” on page 398.

Configuration Commands for a LES-BUS

This section describes the commands for configuring a LES-BUS. Enter the **les-bus** command at the `LE Services config>` prompt. The following example defines a new LES-BUS.

```
LE Services config>les-bus
  (  1) <<< New LES/BUS >>>
  (  2) Test Ethernet Elan
  (  3) Test Token Ring Elan
Choice of LES/BUS [1]?
New ELAN Name (ELANxx) []? elan01
LES-BUS configuration
LES-BUS config for ELAN 'elan01'>
```

The following example allows you to change the configuration of an existing LES-BUS.

```
Choice of LES/BUS [1]? 3
LES-BUS configuration
LES-BUS config for ELAN 'Test Token Ring Elan'>
```

You can enter the following commands:

Table 44. LES-BUS Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds a LES-BUS to a local configuration.
Bus-filter	Accesses the `BUS FILTER config for ELAN 'x'>` command prompt from which you can configure data packet filtering.
Bus-police	Accesses the `BUS POLICE config for ELAN 'x'>` command prompt from which you can configure dynamic traffic management for the BUS.

Table 44. LES-BUS Configuration Commands Summary (continued)

Command	Function
Disable	Disables Broadcast Manager, Bus Filter, BUS-Monitor, Bus Police, LES-BUS, Redundancy, Security, or Source Route Manager.
Enable	Enables Broadcast Manager, Bus Filter, BUS-Monitor, Bus Police, LES-BUS, Redundancy, Security, or Source Route Manager.
List	Lists the operational characteristics of a LES-BUS.
Remove	Removes Broadcast Static Entries, Bus Filter filter items, Bus Police filter items, or LES-BUS.
Set	Sets operational characteristics.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to specify this LES-BUS type, ESI, and selector.

Each LES-BUS must have a unique ELAN name, and the combination of ESI and selector must be unique among all LE components.

Syntax:

add

Example:

```
LES-BUS config for ELAN 'elan01'> add
Select ELAN type
        (1) Token Ring
        (2) Ethernet

Enter Selection: [1]1
Select ESI
        (1) Use burned in ESI

Enter Selection: [1]?1


Selector 0 is generally reserved for use by the LECS,
Selector 1 is generally reserved for use by the LECS interface.

Enter selector [4]?4
Selection "Add LES-BUS" Complete
LES-BUS config for ELAN 'elan01'>
```

Bus-filter

Use the **bus-filter** command to access the `BUS FILTER config for ELAN 'x'>` configuration command from which you can use the following commands to configure bus filters:

Table 45. BUS Filter Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds a bus filter item to a local configuration.
Disable	Disables a Bus filter item.
Enable	Enables a Bus filter item.
Remove	Removes a Bus filter item.
Set	Sets Bus filter parameters.
Show	Displays filter items.

Table 45. BUS Filter Configuration Commands Summary (continued)

Command	Function
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to add data packet filtering.

Syntax:

add ip *filteritem*

mac *address filteritem*

protocol *filteritem*

sliding-window *filteritem*

ip *filteritem*

Adds the specified IP filter item. The following questions will be asked:

IP address type

Specifies whether this IP filter operates on the destination IP address or source IP address. The address is found in the IP header of the packer.

Valid Values: source IP address, destination IP address

Default Value: source IP address

IP subnet

Identifies the subnet or IP address that is to be filtered.

Valid Values: 0.0.0.0 - 255.255.255.255

Default Value: 0.0.0.0

IP subnet mask

Identifies the IP mask used to determine the subnet or IP address of the data packet.

Valid Values: 0.0.0.0 - 255.255.255.255

Default Value: 0.0.0.0

Filter list

Identifies the filter list for which this filter definition is configured.

Valid Values: EXCLUDE, INCLUDE

Default Value: EXCLUDE

Enable this filter?

Identifies whether the filter is to be enabled or disabled.

Valid Values: yes, no

Default Value: yes

Enter filter name

Specifies a name to be associated with this filter.

Valid Values: Any character string up to 32 characters in length

Default Value: None

MAC *address filteritem*

Adds the specified MAC filter item at the specified MAC address. The following questions will be asked:

Mac address type

Specifies whether this filter operates on the destination MAC address or source MAC address.

Valid Values: source MAC address, destination MAC address

Default Value: source MAC address

MAC address

Identifies the MAC address to be ANDed with the data packet's MAC address mask to generate a data packet MAC filter value. This value is then compared with the MAC address to determine the filter action to be taken.

Valid Values: Any valid MAC address

Default Value: FF.FF.FF.FF.FF.FF

MAC address mask

Identifies the MAC address mask to be ANDed with the data packet's MAC address to generate a data packet MAC filter value. This value is then compared with the MAC address to determine the filter action returned.

Valid Values: Any valid MAC address

Default Value: FF.FF.FF.FF.FF.FF

Filter list

Identifies the filter list for which this filter definition is configured.

Valid Values: EXCLUDE, INCLUDE

Default Value: EXCLUDE

Enable this filter?

Identifies whether the filter is to be enabled or disabled.

Valid Values: yes, no

Default Value: yes

Enter filter name

Specifies a name to be associated with this filter.

Valid Values: Any character string up to 32 characters in length

Default Value: None

protocol *filteritem*

Adds the specified protocol filter item. The following questions will be asked:

Protocol

Identifies the protocol type to be managed for BUS filter.

Valid Values:

- IP
- IPX
- NetBIOS
- AppleTalk
- Banyan Vines

- NetBIOS over IP
- IP multicast
- IPX type 20
- BPDU

Default Value: IP

Filter list
Identifies the filter list for which this filter definition is configured.

Valid Values: EXCLUDE, INCLUDE

Default Value: EXCLUDE

Enable this filter?
Identifies whether the filter is to be enabled or disabled.

Valid Values: yes, no

Default Value: yes

Enter filter name
Specifies a name to be associated with this filter.

Valid Values: Any character string up to 32 characters in length

Default Value: None

sliding—window *filteritem*
Adds the specified sliding window filter item. The following questions will be asked:

Filter base
Identifies the base to which the filter offset will be added. When using Token Ring, this information field is the byte following the RIF field. When using Ethernet, this information field is the information following the source address.

Valid Values: mac, info

Default Value: mac

Window filter offset
Identifies the offset from the *filter base* to begin the sliding window test.

Valid Values: 0 - 255

Default Value: 0

Compare value
Specifies the compare value for the sliding window filter. Sliding window data compared with the packet data starting at the specified offset in the packet.

Valid Values: 1 - 32 hexadecimal bytes

Default Value: none

Compare mask
Specifies the compare mask for the sliding window filter. The sliding window mask ANDed with the packet data starting from the *filter base*.

Valid Values: 1 - 32 hexadecimal bytes

Default Value: The same number of X'F' that are specified in the **Compare value**.

Filter list
Identifies the filter list for which this filter definition is configured.

Valid Values: EXCLUDE, INCLUDE

Default Value: EXCLUDE

Enable this filter?
Identifies whether the filter is to be enabled or disabled.

Valid Values: yes, no

Default Value: yes

Enter filter name
Specifies a name to be associated with this filter.

Valid Values: Any character string up to 32 characters in length

Default Value: None

Disable

Use the **disable** command to disable individual filter items.

Choose the filter item to be disabled from the provided list.

Syntax:

disable ip *filteritem*
mac *address filteritem*
protocol *filteritem*
sliding-window *filteritem*

ip *filteritem*
Disables the specified IP filter item.

MAC *address filteritem*
Disables the specified MAC filter item.

protocol *filteritem*
Disables the specified protocol filter item.

sliding—window *filteritem*
Disables the specified sliding window filter item.

Enable

Use the **enable** command to enable individual filter items.

Choose the filter item to be enabled from the provided list.

Syntax:

enable ip *filteritem*
mac *address filteritem*
protocol *filteritem*
sliding-window *filteritem*

ip *filteritem*
Enables the specified IP filter item.

MAC *address filteritem*
Enables the specified MAC filter item.

protocol *filteritem*
Enables the specified protocol filter item.

sliding—window *filteritem*
Enables the specified sliding window filter item.

Remove

Use the **remove** command to remove the specified bus filter item for this LES-BUS. Choose the filter item to be removed from the provided list.

Syntax:

remove	all
	ip *filteritem*
	mac *address filteritem*
	protocol *filteritem*
	sliding-window *filteritem*

all Removes all defined BUS filters.

ip *filteritem*
Removes the specified IP filter item. You will be provided a list of options.

MAC *address filteritem*
Removes the specified MAC filter item at the specified MAC address. You will be provided a list of options.

protocol *filteritem*
Removes the specified protocol filter item. You will be provided a list of options.

sliding—window *filteritem*
Removes the specified sliding window filter item. You will be provided a list of options.

Set

Use the **set** command to set bus filtering for this LES-BUS.

Syntax:

set	default *action*
	preferred *list*

default action
Specifies the default action for the Bus Filter. This is the action taken if no matches occur on any of the defined filter items.

Valid Values: Exclude, Include

Default Value: Exclude

preferred *list*
Sets the list that will be evaluated first (include or exclude).

Valid Values: Exclude, Include

Default Value: Exclude

Show

Use the **show** command to display configured Bus filter items.

Syntax:

show

Example:

```
BUS FILTER config for ELAN 'elan01'> show
Bus Filter Items

Default Action:     EXCLUDE
Preferred List:     EXCLUDE LIST
      Enabled?:     NO

 MAC Filter Items:

(1)Name:mac01
    Address Type: DESTINATION  List: EXCLUDE LIST  Enabled: YES
    Mac Address: 12.34.56.78.90.12
           Mask: FF.FF.FF.FF.FF.FF

 PROTOCOL Filter Items:

(1)Name:protocol01
    Protocol: BPDU              List: EXCLUDE LIST  Enabled: YES

 SLIDING WINDOW Filter Items:

(1)Name:slide01
    Base: MAC   Offset:   0   List: EXCLUDE LIST   Enabled: YES
    Value: 20
     Mask: F0

 IP Filter Items:

(1)Name:ipfilt01
    Address Type: SOURCE       List: EXCLUDE LIST  Enabled: YES
    Address or Subnet: 0.0.0.0
          Subnet Mask: 0.0.0.0
BUS FILTER config for ELAN 'elan02'>
```

Bus-police

Use the **bus-police** command to access the `BUS POLICE config for ELAN 'x'>` configuration command from which you can use the following commands to provide dynamic traffic management for the BUS:

Table 46. BUS Police Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds an entry to the bus police immunity list.
Remove	Removes an entry from the bus police immunity list.
Set	Sets bus police parameters.
Show	Displays bus police immunity list items.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to add a bus police immunity list.

Syntax:

add

Source address
Specifies the source MAC address to be granted immunity.

Valid Values: Any valid MAC address

Default Value: X'FF.FF.FF.FF.FF.FF'

Remove

Use the **remove** command to remove a MAC address from the immunity list.

Syntax:

remove

You will be provided a list of MAC addresses that are on the immunity list. Choose the MAC address you want to remove.

Set

Use the **set** command to set bus police parameters.

Syntax:

set duration
threshold

Duration of Bus Police management
Specifies the installed BUS Police MAC filter duration:

- Temporary indicates that any MAC filter installed by BUS Police is automatically removed by BUS Police if the BUS transmit rate of the offending MAC address falls below the BUS Police **threshold**.
- Permanent indicates that the BUS Police will not remove any installed MAC filters, even if the BUS transmit rate of the offending MAC address later falls below the BUS Police threshold. MAC filters installed by the BUS Police when the duration is set to *permanent* can only be removed through manual intervention.

Valid Values: Temporary or Permanent

Default Value: Temporary

Example: `set bus-police duration`

```
Select Bus Police filter duration
         (1) TEMPORARY
         (2) PERMANENT
Enter Selection: [1]
```

threshold in packets per second

Specifies the BUS Police BUS transmit threshold in packets per second. Packets originating from MAC addresses that exceed this rate during the BUS Monitor Sample Interval will be filtered.

Valid Values: 1 - 100000

Default Value: 50

```
Enter Bus Police Threshold value (1-100000) [50]?
```

Show

Use the **show** command to display the configured Bus police immunity list.

Syntax:

show

Example:

```
BUS POLICE config for ELAN 'elan01'> show

                          Bus Police Immunity List

Threshold:      90
Duration:       Temporary
Enabled?:       Yes

 MAC Address:
 -----------------
 12.34.56.78.90.1A
```

Disable

Use the **disable** command to disable Broadcast Manager, Bus-filter, BUS-Monitor, Bus-police, LES-BUS, Redundancy, Security, or Source Route Manager.

Syntax:

disable bcm ...
bus-filter
bus-monitor
bus-police
les-bus
redundancy
security
source

bcm all *or* **ip** *or* **ipx** *or* **netbios** *or* **ipx-server-farm**
Disables all (or individual) protocols for Broadcast Manager or IPX Server Farm Detection. Broadcast manager is an IBM enhancement to the BUS that reduces broadcast traffic by transforming certain broadcast frames into unicast frames. See “Broadcast Manager” on page 246 for additional information about Broadcast manager. You can disable broadcast manager for all protocols, or for a specific protocol.

bus-filter
Disables data packet filtering.

bus-monitor
Disables BUS-Monitor. BUS Monitor is an IBM enhancement to the BUS that monitors BUS traffic to identify those stations generating the most BUS traffic. See “BUS Monitor” on page 251 for additional information.

bus-police
Disables bus-police, which provides dynamic traffic management for the BUS.

les-bus
Disables LES-BUS. This LES-BUS will be deactivated on the next restart of the router.

redundancy
Disables redundancy. Redundancy is an IBM enhancement to the LES-BUS that allows each LES-BUS to have a backup that will activate if the primary LES-BUS fails. See “LAN Emulation Reliability” on page 248 for additional information.

security
Disables LECS validation of joins.

source route management
Disables Source Route Management for an 802.5 ELAN.

Enable

Use the **enable** command to enable Broadcast Manager, BUS-Monitor, LES-BUS, Redundancy, Security, or Source Route Management.

Syntax:

enable bcm ...
bus-filter
bus-monitor
bus-police
les-bus
redundancy
security
source

bcm all *or* **ip** *or* **ipx** *or* **netbios** *or* **ipx-server-farm**
Enables all (or individual) protocols for Broadcast Manager. Broadcast manager is an IBM enhancement to the BUS that reduces broadcast traffic by transforming certain broadcast frames into unicast frames. See “Broadcast Manager” on page 246 for additional information about Broadcast manager. You can enable broadcast manager for all protocols, or for a specific protocol.

Note: You cannot enable the Broadcast Manager while the BUS is in Adapter or VCC-Splice mode.

When *ipx-server-farm* and *BCM IPX* are enabled, BCM IPX detects the presence of at least ***server-farm-threshold*** IPX servers behind a single

LEC. When a server farm is detected, BCM IPX subsequently transmits a single broadcast to the LEC that is proxying for the server farm.

bus-filter
Enables data packet filtering. This lets the BUS use the configured filters to limit data traffic propagated across the ELAN, improving security from unwanted broadcast attacks, improving bandwidth utilization by limiting data traffic, and centralizing filter controls in a single location to facilitate filtering management.

bus-monitor
Enables BUS-Monitor. BUS Monitor is an IBM enhancement to the BUS that monitors BUS traffic to identify those stations generating the most BUS traffic. See “BUS Monitor” on page 251 for additional information.

Note: You cannot enable the BUS-Monitor while the BUS is in VCC-Splice mode.

bus-police
Enables BUS-police. BUS-police uses BUS Monitor to provide dynamic BUS traffic management. BUS data traffic is sampled and filters are dynamically installed for devices that exceed the value of the **BUS usage threshold** configuration parameter.

Note: You can enable BUS-Police only if BUS Monitor is enabled.

les-bus
Enables LES-BUS. This LES-BUS will be activated on the next restart of the router.

redundancy
Enables redundancy. Redundancy is an IBM enhancement to the LES-BUS that allows each LES-BUS to have a backup that will activate if the primary LES-BUS fails. When the Peer Redundancy option is enabled at the primary LES-BUS, the back-up LES-BUS may remain active after the Primary LES-BUS recovers. See “LAN Emulation Reliability” on page 248 for additional information.

Example:

```
LES-BUS config for ELAN 'elan01'> enable redundancy
     ( 1) Primary LES-BUS
     ( 2) Backup LES-BUS
Redundancy Role [1]?
Enable Peer Redundancy Option? [No]?
ATM address of backup les-bus in 00.00.00.. form [ ]?39.84.0F.00.00.00.00.00.00.00.00.02.22.33.44.55.66.77.02
LES-BUS config for ELAN 'elan01'>
```

security
Enables LECS validation of joins. If enabled, the LES-BUS communicates with the LECS across the LES-LECS Security Interface in order to validate each LE Client’s request to join the ELAN. The LES-LECS Security Interface for this ATM Interface must be enabled (see “Configuration Commands for Security for ELANs” on page 398).

source route management
Enables Source Route Management for an 802.5 ELAN. SRM can transform spanning tree explorer and all routes explorer packets into specifically routed frames. SRM operates only on those frames managed by BCM IP or BCM NetBIOS. See “BCM Support for Source Route Bridging” on page 248 for additional information.

Note: You cannot enable Source Route Management while the BUS is in Adapter or VCC-Splice mode.

List

Use the **list** command to list LES-BUS configuration values for this ELAN.

Syntax:

list

As part of the prompt in the following example, the expression "--More--" appears numerous times. When this happens, you have three options:

- Press the **Enter** key. This is useful if you want to examine your configuration values one line at a time (just press the **Enter** key when you are ready to view the next line of values).
- Press the space bar to display an entire page of your configuration data. This option was used in the following example.
- Enter the character **q** to discontinue the list and return to the previous prompt.

Example:

```
LES-BUS config for ELAN 'elan01'> list

LES-BUS Detailed Configuration
Name:  CFG
   LES-BUS Enabled/Disabled:                  Enabled
   ATM Device number:                         0
   End System Identifier (ESI):               Use Burned in ESI
   Selector Byte:                             0x03
   ELAN Type:       (S2)                      Ethernet
   Max Frame Size:  (S3)                      1516
   Control Timeout: (S4)                      120
   Max Frame Age:   (S5)                      1
   ELAN Identifier: (S7)                      0 (not configured)
   Mcast Send Disconnect Timeout: (S9)        60
   LECID Range Minimum:                       0x0001
   LECID Range Maximum:                       0xFEFF
   Validate Best Effort Peak Cell Rate (PCR): No
   Control Distribute VCC Traffic Type:       Best Effort VCC
   Control Distribute VCC PCR in Kbps:        155000
   Control Direct VCC Max Reserved Bandwidth: 0
   Multicast Forward VCC Traffic Type:        Best Effort VCC
   Multicast Forward VCC PCR in Kbps:         155000
   Multicast Send VCC MAX Reserved Bandwidth: 0
    -LES-BUS Options-
   BUS Mode:                                  Adapter
   Security (LECS Validation of Joins):       Disabled
   Partition LE_ARP_REQUEST Forwarding Domain: Yes
   LE_ARP RESPONSE Destination:               One client
   Partition Unicast Frame Domain:            Yes
   Redundancy:                                Enabled
   Peer Redundancy:                           Enabled
   Redundancy Role:                           Primary LES-BUS
   ATM address of Backup LES-BUS:  39999999999999000099990200004AC47390902
   ATM address trace filter value: 00000000000000000000000000000000000000000
   ATM address trace filter mask:  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
    -BUS Monitor Configuration-
   Monitor Host Usage of BUS:                 Disabled
   # Top Hosts to Record:                     10
   # Seconds in each sample interval:         10
   # Seconds between sample intervals:        1800
   Frame sampling rate:                       1 out of 10
    -Broadcast Manager Configuration-
   IP BCM:                                    Disabled
   IPX BCM:                                   Disabled
   NetBIOS BCM:                               Disabled
   BCM IP Cache Aging Time:                   5
   BCM IPX Cache Aging Time:                  3
   BCM NetBIOS Cache Aging Time:              15
   BCM IPX Maximum Forwarding List:           50
   BCM IPX Server Farm Detection:             Disabled
   BCM IPX Server Farm Threshold:             20
   No BCM IPX Static Entries defined
    - Bus Filter Configuration-
   BUS Filter enabled:                        enabled
   BUS Filter's Preferred List                EXCLUDE list
   BUS Filter's Default Action                EXCLUDE
   - Bus Police Configuration-
   Bus Police Enabled:                        Enabled
   Bus Police Filter Duration:                TEMPORARY
   Bus Police Threshold (packets/sec):         50
LES-BUS config for ELAN 'elan01'>
```

Remove

Use the **remove** command to remove broadcast static entries or a LES-BUS pair.

Syntax:

remove broadcast

les-bus

broadcast
Removes static entries defined for IPX Broadcast Manager.

les-bus
Deletes the LES-BUS configuration.

Example: `remove broadcast`

```
Choose static entry to remove
        (1) 12345678901234567890123456789012345678901234567890/FFFFFFFFFFFF
        (2) 21234567890123456789012345678901234567890123456789/FFFFFFFFFFFF
        (3) 32123456789012345678901234567890123456789012345678/FFFFFFFFFFFF
        (4) < CANCEL >

Enter Selection:  [1]? 4
Remove operation canceled.
```

Set

Use the **set** command to set operational characteristics associated with this ELAN.

Syntax

set
address
broadcast *static entries*
bus-mode
bus-monitor *settings*
control *timeout*
elan *identifier*
frame-age
frame-size
ip *broadcast cache age*
ipx-broadcast *cache age*
ipx-maximum *size of forwarding list*
ipx-server-farm *threshold*
le-arp *response destination*
lecid *range*
local *segment number*
multicast-send-disconnect-timeout
netbios *broadcast cache age*
partition *forwarding domain*
trace
traffic *type*

address
Specifies the End System Identifier (ESI) and selector components of the LES-BUS's ATM address. For more information on addressing in ATM and

on the ATM address of the LE components on the server see “Addressing in ATM” on page 235 and “ATM Addresses of LAN Emulation Components” on page 236.

Example: `set address`

```
Select ESI
        (1) Use burned in ESI

Enter Selection:  [1]?1
Selector 0 is generally reserved for use by the LECS,
Selector 1 is generally reserved for use by the LECS Interface.

Enter selector [7]?7
Selection "Set Address" Complete
LES-BUS config for ELAN 'elan01'>
```

broadcast

Defines static entries for IPX Broadcast Manager (BCM). IPX BCM dynamically discovers IPX routers and servers in the IPX network containing this ELAN by monitoring traffic sent to the BUS for IPX advertisements.

Uses for static targets are:

- Any device that requires reception of IPX advertisements that does not transmit advertisements must be configured as a static target. An example would be a station running software that discovers IPX network topology by monitoring IPX advertisements. Broadcast Manager for IPX is not aware of this “quiet” station without a static target definition of its MAC address and the address of the representing LEC.
- Use to hard-code a particular LEC as representing an IPX Server Farm.
- Use to exclude a LEC from being detected as a Server Farm by automatic IPX Server Farm Detection.

If the IPX Server Farm Detection function is disabled on this LES/BUS, you can use a static target effectively when many IPX routers and servers are represented by a single LEC. By configuring a static target with the ATM address of the LEC, but with a broadcast MAC address of all X'F's, all IPX routers and servers behind the LEC receive a single broadcast advertisement rather than multiple unicast advertisements.

If BCM IPX Server Farm Detection is enabled and you wish to prevent a particular LEC from being treated by BCM IPX as a Server Farm, configure a BCM static target with the LEC's ATM address and a MAC address of 00.00.00.00.00.00. This forces BCM IPX to send frames managed by BCM as multiple unicast frames to each downstream IPX router and server detected behind this LEC, even if the number of routers and servers detected exceeds the *BCM IPX Server Farm Threshold*.

Example: `set broadcast`

```
Enter ATM address in 00.00.00.. form [ ]? 00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.01
Enter MAC address in 00.00.00.. form [FF.FF.FF.FF.FF.FF]?FF.FF.FF.FF.FF.FF
Selection "Set Broadcast Static Entry" Complete
LES-BUS config for ELAN 'elan01'>
```

bus-mode *mode*

Sets the bus mode for this LES-BUS. The different modes trade intelligence for increased forwarding speed of the LES-BUS. The modes are:

System
All BUS features are available and can be enabled or disabled. Frames received by the BUS are moved into system memory for analysis before transmission.

Adapter
Frames received for the BUS are not moved into system memory but remain on the ATM adapter until transmitted. If the ELAN is operational in this mode, the Broadcast Manager and Source Route Management are unavailable and cannot be enabled.

All BUS frames for token-ring ELANs are counted as multicast frames.

VCC-Splice
The client's multicast send VCC to the BUS is "spliced" to the multicast forward VCC, allowing the ATM adapter to transmit received frames from one VCC to its spliced VCC pair without notifying the system processor. Statistics are not maintained by the BUS.

Notes:

1. Unicast partitioning must be disabled to set the BUS mode to VCC-Splice.
2. If the ELAN is operational in this mode, the Broadcast Manager and Source Route Management are unavailable and cannot be enabled.
3. BUS Monitor is unavailable in VCC-Splice mode.

Default value: Adapter.

bus-monitor *settings*
Specifies sample interval, sampling rate, inter-sample sampling time, and the number of MAC addresses to record for BUS Monitoring. The BUS Monitor parameters control how often BUS Monitor samples frames. More frequent sampling leads to more accurate results, but also requires more processing time at the BUS.

Example: `set bus-monitor duration`

```
Duration of sample interval in seconds (1-600) [10]?10
Selection "Set BUS monitoring sample interval" Complete
LES-BUS config for ELAN 'elan01'>
```

Example: `set bus-monitor sample`

A value of 10 means 1 out of every 10 frames is sampled.

```
Frame sampling rate (1-1000) [10]?10
Selection "Set the sampling rate" Complete
LES-BUS config for ELAN 'elan01'>
```

Example: `set bus-monitor time`

```
Number of seconds between sample intervals (2-7200) [1800]?15
Selection "Set BUS monitoring inter-sample time" Complete
LES-BUS config for ELAN 'elan01'>
```

Example: `set bus-monitor top`

```
Number of top MAC addresses to record (1-100) [10]?10

Selection "Set number of top MAC addresses to record" Complete
LES-BUS config for ELAN 'elan01'>
```

control *timeout*

Sets the control timeout, in seconds, for the LE Server. This is the timeout used for many of the response/request exchanges. This parameter maps to the S4 parameter in the *ATM Forum LAN Emulation Over ATM Specification*. A smaller control timeout may lead to quicker response times, but may also lead to unnecessary retransmissions. This parameter should be coordinated with the control timeout of LE clients joining this LES.

Example: `set control`

```
Control Timeout (10-300): [120]?120
Selection "Set Control Timeout" Complete
LES-BUS config for ELAN 'elan01'>
```

elan *identifier*

This parameter sets the identifier for this elan that is returned to LECs in join response and is used by LECs to de-multiplex LLC-multiplexed VCCs.

Valid Values:

0 - X'FFFFFFFF'

Default Value:

0

frame-age

Sets maximum frame age. The BUS must discard a frame if it has not transmitted the frame to all relevant VCCs within the Maximum Frame Age following the BUS's receipt of the frame. This parameter maps to the S5 parameter in the *ATM Forum LAN Emulation Over ATM Specification*.

Example: `set frame-age`

```
Maximum Frame Age (1-4): [1]?1
Selection "Set Maximum Frame Age" Complete
LES-BUS config for ELAN 'elan01'>
```

frame-size

Sets maximum frame size. The maximum size of an AAL-5 Service Data Unit (SDU) that the LE Service can guarantee not to drop for being too large. Also the minimum AAl-5 SDU size that every LE Client must be able to receive. This parameter maps to the S3 parameter in the *ATM Forum LAN Emulation Over ATM Specification*

Example: `set frame-size`

```
Maximum Frame Size:
        (1) 1516
        (2) 1580
        (3) 4544
        (4) 9234
        (5) 18190

Enter Selection:  [2]?2
Selection "Set Maximum Frame Size" Complete
LES-BUS config for ELAN 'elan01'>
```

ip *broadcast cache age*

Sets IP Broadcast cache age in minutes. This is the maximum number of minutes an IP entry will be kept without re-verification of its location.

Example: `set ip`

```
IP cache age in minutes (2-20): [5]?5
Selection "Set IP broadcast cache age" Complete
LES-BUS config for ELAN 'elan01'>
```

ipx-broadcast *cache age*

Sets IPX Broadcast cache age in minutes. This is the maximum number of minutes an IPX entry will be kept without re-verification of its location.

Example: `set ipx-broadcast`

```
IPX cache age in minutes (1-10): [3]?3
Selection "Set IPX broadcast cache age" Complete
LES-BUS config for ELAN 'elan01'>
```

ipx-maximum *size of forwarding list*

Sets the maximum number of entries that BCM IPX will maintain in its forwarding list. The value of this parameter must be > the value of *ipx-server-farm threshold*.

Note: This parameter sets an upper limit to the device's performance, so use caution when increasing this limit. BCM IPX's forwarding list consists of one entry for each:

- BCM static target currently active on the ELAN
- LEC detected to be a server farm if IPX Server Farm Detection is enabled
- Dynamically discovered IPX router or server in the IPX network containing this ELAN.

  Individual routers and servers represented by a detected server farm or BCM static target do not count toward this limit.

Each broadcast frame managed by BCM IPX is individually transmitted to each member on the forwarding list. If the number of members ever exceeds the maximum, BCM IPX automatically shuts down, allowing BUS to forward IPX broadcasts as usual.

Example: `set ipx-maximum`

```
IPX Maximum Size of Forwarding List (5-65535): [50]? 60
Selection "Set IPX Maximum Size of Forwarding List" Complete
```

ipx-server-farm *threshold*

Sets the minimum number of IPX routers and servers behind a given LEC required for BCM IPX Server Farm Detection to detect a server farm. When a server farm is detected, BCM IPX broadcasts a managed frame to each LEC representing a server farm, rather than transmitting multiple unicast frames to each device in the server farm. The value of this parameter must be ≤ the value specified for *ipx-maximum size of forwarding list*. See "Broadcast Manager" on page 246 for additional information.

Valid Values:

2 - 65535

Default Value:

20

lecid *range*

Sets bounds on the range of lecids used by this LES. By configuring a lecid range, you can guarantee that all LESs within a Super ELAN use a disjoint set of lecids. Maintaining lecid uniqueness within a Super ELAN is required if any clients filter data-direct VCCs based on lecid, or if any clients do not implement the (C22) path switch delay timer.

This parameter can also be used to limit the number of clients served by this LES-BUS.

local-segment-number

This parameter sets the local segment identifier for token-ring ELANs.

Valid Values:

0 - X'0FFF'

Default Value:
0

multicast-send-disconnect-timeout
This parameter sets the maximum number of seconds that a LEC may be connected to the LES (using Control VCCs) but not connected to the BUS (using Multicast VCCs). If a LEC remains in such a state for this amount of time, the LES must terminate the ELAN membership of the LEC.

Valid Values:
10 - 300 seconds

Default Value:
60

netbios *broadcast cache age*
Sets NetBIOS cache age in minutes. This is the maximum number of minutes an NetBIOS will be kept without re-verification of its location.

Example: `set netbios`

```
NetBIOS cache age in minutes (10-20): [15]?12
Selection "Set NetBIOS broadcast cache age" Complete
LES-BUS config for ELAN 'elan01'>
```

partition *forwarding domain*
Partitions the *control distribute* or *multicast forward* VCCs.

Proxy clients are placed on one Control Distribute VCC and all other clients are placed on another Control Distribute VCC. Partitioning the VCCs reduces nuisance traffic at many clients because non-proxy LECs do not receive proxy LEC traffic, and vice-versa. However, some frames must now be forwarded on two VCCs. In general, partitioning the VCCs is recommended.

The **set partition address** command partitions the control distribute VCC into a “proxy control distribute” VCC and a “non-proxy control distribute” VCC.

Example: `set partition address`

```
Partition address resolution forwarding domain [yes]yes
Selection "Partition address resolution forwarding domain" Complete
LES-BUS config for ELAN 'elan01'>
```

The **set partition unicast** command partitions the multicast forward VCC into a “proxy multicast forward” and a “non-proxy multicast forward” VCC.

Note: Unicast partitioning can not be set to *yes* when BUS Mode is set to *VCC-Splice*.

Example: `set partition unicast`

```
Partition unicast frame forwarding domain [yes]?no
Selection "Partition unicast frame domain" Complete
LES-BUS config for ELAN 'elan01'>
```

trace mask *or* **value**
Sets trace filter mask or trace filter value for ATM address. For each VCC, if the ATM address of the entity at the other end of the VCC matches the ATM-address-value on all bits set by the ATM-address-mask, then packet tracing *can* be performed on that VCC. For packet tracing to occur, enable it in the ELS subsystem (for additional information, refer to “Chapter 13. Using the Event Logging System (ELS)” on page 145.

Example: `set trace mask`

```
LES-BUS config for ELAN 'elan01'>set trace mask
ATM address trace filter mask [FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF]?
Selection "Set ATM address trace filter mask" Complete
LES-BUS config for ELAN 'elan01'>set trace value
ATM address trace filter value [00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00]?
Selection "Set ATM address trace filter value" Complete
```

traffic *type pcr*

Sets traffic characteristics:

- *set traffic control* sets traffic characteristics of the “control distribute” VCC.

  Example: `set traffic control`

  ```
  Traffic type
          (1) Best Effort
          (2) Reserved Bandwidth

  Enter Selection:  [1]?1

  Peak cell rate in Kbps (1 - 155000) [155000]?155000

  Selection "Set Control distribute VCC" Complete
  LES-BUS config for ELAN 'elan01'>
  ```

- *set traffic maximum control* or *set traffic maximum multicast* sets the maximum reserved bandwidth allowed either on control direct or on multicast send reserved bandwidth VCCs. Reserved bandwidth VCCs with requested bandwidth higher than the maximum specified by this command are rejected.

  Example: `set traffic maximum control`

  ```
  Maximum reserved bandwidth in Kbps (0 - 155000) [0]?100000
  Selection "Set Control Direct VCC maximum reserved bandwidth" Complete
  LES-BUS config for ELAN 'elan01'>
  ```

- *set traffic multicast* sets traffic characteristics of the multicast forward VCC.

  Example: `set traffic multicast`

  ```
  Traffic type
          (1) Best Effort
          (2) Reserved Bandwidth

  Enter Selection:  [1]?1

  Peak cell rate in Kbps (1 - 155000) [155000]?90000

  Selection "Set Multicast Forward VCC" Complete
  LES-BUS config for ELAN 'elan01'>
  ```

- *set traffic validate* determines whether the LES-BUS is to validate the peak cell rate specified on incoming control direct or multicast send VCCs. When you specify this command, the LES-BUS rejects all control direct or multicast send VCCs that specify a peak cell rate that is greater than the maximum data rate of the ATM interface.

  Example: `set traffic validate`

  ```
  Validate peak cell rate of best effort VCCs [no]no
  Selection "Validate Peak Cell Rate of best effort VCCs" Complete
  LES-BUS config for ELAN 'elan01'>
  ```

Configuration Commands for a LECS

Enter the **lecs** command at the `LE Services config>` prompt to enter the `LECS config>` environment where you initiate configuration for the individual ELANS for your network.

Table 47. LECS Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Access-control	Provides ATM address screening for security at the LECS.
Add	Adds a LECS to the static configuration of the ATM network.
Database-Synchronization	Configures database-synchronization
Elans	Configures the ELANs under the administrative domain of the LECS.
List	Lists the configuration of the LECS on the MSS Server.
Policies	Configures the policies guiding this LECS.
Remove	Removes the LECS from the static configuration of the ATM network.
Search	Lets you use “search keys” to simplify configuration management.
Set	Sets operational characteristics of the LECS.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Access-control

The **access-control** command puts you in the LECS Access Control configuration environment. These commands allow you to configure a list of ATM address prefixes (1 - 20 octets) which are not allowed access to the LECS configuration database. All LECS connection attempts and configuration requests from matching ATM addresses are rejected. The LECS Access Control configuration environment is characterized by the `LECS Access Control config>` prompt.

Syntax:

access-control

Example:

```
LECS config> access-control
LECS Access Control config>
```

For additional information, see “Configuration Commands for the Access Control of a LECS” on page 380.

Add

The **add** command adds a LECS to the static configuration of the MSS Server. You are prompted to select the ESI to be used in the ATM address of the LECS. You are also asked to select whether to activate error logging on the LECS subsystem. For further information on error logging, see “ELS Configuration Commands” on page 165.

Syntax:

add

Example:

```
LECS config> add
  (  1) Use burned in ESI
End system identifier [1]?yes
LECS added to configuration
Enable standard Error Logging System for LECS? [Yes] Y
Standard ELS activated for LECS
LECS config>
```

Database-Synchronization

The **database-synchronization** command accesses the `LECS Database Sync config>` command prompt from which you can configure remote LECS addresses to participate in database synchronization. See “LECS Database Synchronization” on page 252 for additional information.

Syntax:

database-synchronization

Example:

```
LECS config> database-sync
LECS Database Sync config>
```

The following commands are available at the `LECS Database Sync config>` prompt.

Table 48. LECS Database Synchronization Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add-user-defined	Manually adds a LECS ATM address to the database synchronization list.
Add-via-ilmi	Adds the LECS ATM addresses retrieved via ILMI to the database synchronization list.
Disable	Disables a LECS ATM address from participation in database synchronization.
Enable	Enables a LECS ATM address to participate in database synchronization.
List	Lists the database synchronization configuration.
Remove	Removes a LECS ATM address from participation in database synchronization.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add-user-defined

The **add-user-defined** command allows a remote LECS to be manually added to the list of LECSs participating in database synchronization.

Syntax:

add-user-defined

Example:

```
LECS Database Sync config> add-user-defined
Remote LECS ATM address [] 399999999999990000999901021111111111111100
Added remote LECS ATM address successfully
LECS Database Sync config>
```

Remote LECS ATM address

Specifies the ATM address of an external MSS LECS whose LECS configuration is to be overwritten with the configuration for this LECS.

Valid Values: Any valid ATM address

Default Value: None

Add-via-ilmi

The **add-via-ilmi** command adds the LECS ATM addresses retrieved from the attached ATM switch via ILMI to the list of LECSs participating in database synchronization.

Syntax:

add-via-ilmi

Example:

```
LECS Database Sync config> add-via-ilmi
Remote LECS ATM address
    (1) All addresses retrieved from switch
    (2) 39.99.99.99.99.99.99.00.00.99.99.01.02.11.11.11.11.11.11.00
Enter Selection: [1]?
Selection "LECS remote ATM address addition" Complete
LECS Database Sync config>
```

Disable

The **disable** command disables a remote LECS from participation in database synchronization.

Syntax:

disable

Example:

```
LECS Database Sync config> disable
 Remote LECS ATM Address
    (1) All
    (2) 39.99.99.99.99.99.99.00.00.99.99.01.02.11.11.11.11.11.11.00
Enter Selection:  [1] 2
LECS Database Sync disabled:
    39.99.99.99.99.99.99.00.00.99.99.01.02.11.11.11.11.11.11.00

Selection "LECS remote ATM address disable" Complete
LECS Database Sync config>
```

Enable

The **enable** command enables a remote LECS to participate in database synchronization.

Syntax:

enable

Example:

```
LECS Database Sync config> enable
Remote LECS ATM Address
  (1) All
  (2) 39.99.99.99.99.99.99.00.00.99.99.01.02.11.11.11.11.11.11.00
Enter Selection:  [1] 2
LECS Database Sync enabled:
   39.99.99.99.99.99.99.00.00.99.99.01.02.11.11.11.11.11.11.00
Selection "LECS remote ATM address enable" Complete
LECS Database Sync config>
```

List

The **list** command displays the ATM addresses of the remote LECS that are participating in database synchronization.

Syntax:

list

Example:

```
LECS Database Sync config> list
Remote LECS Databases to Synchronize
Enabled  Remote LECS Atm Address
=======  ============================================================
    Yes  39.99.99.99.99.99.99.00.00.99.99.01.02.11.11.11.11.11.11.00

LECS Database Sync config>
```

Remove

The **remove** command removes a remote LECS from participation in database synchronization.

Syntax:

remove

Example:

```
LECS Database Sync config> remove
 Remote LECS ATM Address
    (1) All
    (2) 39.99.99.99.99.99.99.00.00.99.99.01.02.11.11.11.11.11.11.00
Enter Selection:  [1] 2
LECS Database Sync removed:
     39.99.99.99.99.99.99.00.00.99.99.01.02.11.11.11.11.11.11.00

Selection "LECS remote ATM address remove" Complete
LECS Database Sync config>
```

Elans

Type the **elans** command to enter the LECS ELANs Configuration environment. In this environment, you configure all ELANs under the administrative domain of the LECS. This environment is characterized by the `LECS ELANS config>` prompt.

Syntax:

elans

Example:

```
LECS config> elans
Configuration of ELANs for LECS
LECS ELANS config>
```

For a description of commands used in the `LECS ELANS config>` environment, see “Configuration Commands for ELANs at the LECS” on page 382.

List

The **list** command displays the configuration of the LECS. The various configuration parameters are described under “Set” on page 379.

Syntax:

list

Example:

```
LECS config>list
LECS Detailed Configuration
   Lecs is                                      Enabled
   ATM Device number:                           0
   ESI:                                         Use burned in ESI
   Selector:                                    0x00
   Validate Best Effort PCR:                    No
   Configuration Direct Max Reserved BW (Kbps): 0
   Maximum number of simultaneous VCCs:         128
   Idle VCC Timeout (in seconds):               60
   Trace ATM address value: 00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00
   Trace ATM address mask:  FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF
   Automatic Database Synchronization:          No
   Allow Config From Remote LECS:               No
```

Policies

The **policies** command puts you in the LECS Policies Configuration environment. In this environment, you configure the policies used to guide the LECS operation. The LECS Policies Configuration environment is characterized by the `LECS Policies config>` prompt.

Syntax:

policies

Example:

```
LECS config> policies
LECS Policies config>
```

For additional information, see “Configuration Commands for the Policies of a LECS” on page 396.

Search

The **search** command provides “search keys” to simplify configuration management. Each search key represents some unique aspect of LE Servers or LE Clients (ATM address, MAC address, name of ELAN, and so on). Search keys can be used to determine which ELAN a particular LES is serving, or to which LES a certain policy value is assigned.

Syntax:

search	atm
	les
	mac

name

route

Example: `search mac`

```
LECS config> search mac
Enter MAC address using its natural bit-order
MAC address to search for [ ]?11.11.11.11.11.11
MAC address 11.11.11.11.11.11
   for LES 00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00
      for ELAN 'lgrove01'
LECS config>
```

Set

The **set** command lets you change the operational characteristics of the LECS.

Syntax:

set

- address
- auto database synchronization
- enable-disable
- maximum number of VCCs
- remote configuration
- reserved bandwidth maximum
- trace
- validate best effort peak cell rate
- vcc idle time

Example:

```
LECS config> set address
End system identifier
        (1) Use burned in ESI

Enter Selection: [1]?
Selector 0 is generally reserved for the LECS and
selector 1 is generally reserved for the LECS interface.
Selector [0]?4
Selector of LECS' ATM address is 4
Selection "LECS address modification" Complete
LECS config>
```

Address

Changes the address of the LECS. This is the local ATM address of the LECS. At the ATM switches, you may also configure the well-known LECS address to be associated with this local ATM address. See “Addressing in ATM” on page 235 for additional information about addressing.

Auto database synchronization

Specifies whether the LECS database synchronization will be done automatically when LECS comes up or only at the user’s command. When in Auto mode, the LECS external network configuration will be written to all LECS addresses in the configured list whenever the server is rebooted or the LECS restarted using the `talk 6` parameters. As in the case of manual synchronization, the remote LECS will be restarted if configuration is successfully written.

Valid Values: Yes or No

Default Value: No

Enable/Disable
Enables or disables the LECS. If the LECS is disabled, it will not be started the next time the router is restarted.

Maximum number of VCCs
Maximum number of configuration direct VCCs that the LECS supports at one time. If the actual number of VCCs to the LECS exceeds this number, the LECS releases *all* VCCs that have not been used in the number of seconds specified by the VCC idle time (described below).

Remote configuration
Specifies whether the LECS is allowed to have its LECS database configuration remotely overwritten by another LECS during LECS database synchronization.

Valid Values: Yes or No

Default Value: No

Reserved bandwidth maximum
Maximum bandwidth (in Kbps) that the LECS accepts on any reserved bandwidth configuration direct VCC.

Trace *value* **or** *mask*
Each LE component supports packet tracing. You can specify an ATM address filter for packet tracing. For each VCC, if the ATM address of the entity at the other end of the VCC matches the ATM-address-value on all bits set by the ATM-address-mask, then packet tracing *can* be performed on that VCC. For packet tracing to occur, enable it in the ELS subsystem (for additional information, refer to “Chapter 13. Using the Event Logging System (ELS)” on page 145.

Validate best effort peak cell rate
Answer **yes** or **no**.

When you configure the LECS to validate best effort PCR, the peak cell rate (specified while setting up each VCC) is examined. If the peak cell rate is greater than the maximum date rate of the ATM interface, the requested VCC is rejected.

VCC idle time
Number of seconds (of idle time) before LECS releases VCCs that have not been used when the number of VCCs exceeds the number that the LECS supports. (See also “Maximum number of VCCs” above.)

Configuration Commands for the Access Control of a LECS

Use the **access-control** command to configure ATM address screening at the LECS. The following commands can be issued at the `LECS Config>` command prompt:

Table 49. Access Control Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds an ATM address to the screening list.
Disable	Disables ATM address screening.

Table 49. Access Control Configuration Commands Summary (continued)

Command	Function
Enable	Enables ATM address screening.
List	Displays the ATM address screening list.
Remove	Removes an ATM address from the screening list.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

The **add** command adds an ATM address prefix (1 - 20 octets) to the access control screening list.

Syntax:

add ***atm-address-prefix***

Example:

```
LECS Access Control config>add
Suspect ATM address choice []? 39999999999999000099990101
Added suspect ATM address '39.99.99.99.99.99.99.00.00.99.99.01.01' successfully
LECS Access Control config>
```

Disable

The **disable** command disables an address prefix for access control screening.

Syntax:

disable ***atm-address-prefix***

Enable

The **enable** command enables an address prefix for access control screening.

Syntax:

enable ***atm-address-prefix***

List

The **list** command displays the access control screening list.

Syntax:

list

Example:

```
LECS Access Control config>list

Suspect ATM addresses for LECS

Enabled  Suspect Atm Address
=======  ==================================================
    Yes   39.99.99.99.99.99.99.00.00.99.99.01.01

LECS Access Control config>
```

Remove

The **remove** command removes an ATM address prefix from the access control screening list.

Syntax:

remove ***atm-address-prefix***

Configuration Commands for ELANs at the LECS

The primary function of the LECS is to assign clients to LESs that serve ELANs. You enter commands at the `LECS ELANs config>` prompt to configure all of the ELANs under the administrative control of the LECS. Before *any* client for a particular ELAN can use this LECS, information on that ELAN must be configured on this LECS. Even if an ELAN is served by a local LES-BUS, the ELAN information must be configured here if the LECS is to refer any clients to that ELAN.

To configure ELANs under the administrative domain of the LECS, enter the **elans** command at the `LECS config>` prompt:

```
LECS config> elans
Configuration of ELANs for LECS
LECS ELANs config>
```

You can enter the following commands at the `LECS ELANs config>` prompt:

Table 50. LECS ELANs Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds an ELAN to the static configuration administered by the LECS.
List	Summarizes the ELANs that are under the administrative control of the LECS.
Remove	Removes an ELAN from the static configuration administered by the LECS.
Select elan	Selects an ELAN for more detailed configuration.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

The **add** command adds an ELAN to the static configuration administrated by the LECS. You will be prompted for the ELAN name, type, and maximum frame size.

Syntax:

add

Example:

```
LECS ELANs config> add
Name of ELAN [ ]? cary02
Type of ELAN
     (1) Ethernet
     (2) TokenRing
Enter Selection:  [2]? 2
Maximum frame size of ELAN
        (1) 1516
        (2) 4544
        (3) 9234
        (4) 18190
        (5) 1580
```

```
Enter Selection:  [2]? 2
ELAN 'cary02' added
Selection "ELAN addition" complete
LECS ELANs config>
```

List

The **list** command summarizes the ELANs under the administrative domain of the LECS.

Syntax:

list

Example:

```
LECS ELANs config> list

ELAN Listing...
                                    Name   Type   Packet Size   Enabled
==================================   ====   ====   ===========   =======
                                   ELAN1   TokR          4544   Yes
                                   ELAN2   TokR          4544   Yes
LECS ELANs config>
```

Remove

The **remove** command prompts you remove an ELAN from the static configuration administered by the LECS. After you enter your choice, a confirmation is displayed.

Syntax:

remove

Example:

```
LECS ELANs config>remove
Choice of ELAN
        (1) All
        (2) cary01
        (3) cary02
        (4) < CANCEL >

Enter Selection:  [1]? 3
Removed ELAN 'cary02'
Selection "ELAN removal" Complete
```

Select

The **select** command prompts you to select an ELAN for additional (detailed) configuration.

Syntax:

select

Example:

```
LECS ELANS config> select
  (  1) cary01
  (  2) lgrove01
  (  3) lgrove02
  (  4) lgrove03
Choice of ELAN [1]?2
ELAN 'lgrove01' selected for detailed configuration

Selected ELAN 'lgrove01'>
```

Configuring ELANs at the LECS

Additional information on detailed configuration can be found at “Configuration Commands for ELAN Detailed Configuration”.

Configuration Commands for ELAN Detailed Configuration

This section provides examples of configuring an ELAN in detail. It assumes that you already have completed the configuration requirements outlined in “Configuration Commands for ELANs at the LECS” on page 382. Detailed configuration is done from the `ELAN 'elan-name' selected for detailed configuration>` prompt. For example:

```
LE Services config> lecs
Lan Emulation Configuration Server configuration
LECS config> elans
Configuration of ELANs for LECS
LECS ELANs config> select
  (  1) cary01
  (  2) lgrove01
  (  3) lgrove02
  (  4) lgrove03
Choice of ELAN [1]?2
ELAN 'lgrove01' selected for detailed configuration
Selected ELAN 'lgrove01'>
```

Use the following commands for detailed configuration:

Table 51. LECS ELANs Detailed Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Les	Manages the LESs that serve the selected ELAN.
List	Lists the configuration of the selected ELAN.
Policy	Manages the policy values assigned to the LESs serving the selected ELAN.
Set	Enables or disables the selected ELAN, and manages the name, type, and maximum frame size of the ELAN.
ELAN-tlv	Manages TLVs associated with the selected ELAN.
LEC-tlv	Allows TLVs to be associated with an ELAN policy that is identified by ATM address, MAC address, route descriptor, or ELAN name.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Les

Table 52. Selected ELAN LES Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds a LES address to the ELAN static configuration administered by the LECS.
Disable	Disables a LES address in the ELAN static configuration administered by the LECS.
Enable	Enables a LES address in the ELAN static configuration administered by the LECS.
List	Summarizes the LES configuration for the ELANs that are under the administrative control of the LECS.
Remove	Removes a LES address.
Set	Sets ELAN static configuration parameters.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Use the **les** command to manage the LES ATM addresses that represent LESs serving the selected ELAN. The ATM address of each LES serving this ELAN must exist here. Each LES ATM address can consist of two addresses, a primary LES address and a backup LES address. The backup LES address serves as a hot standby LES that activates when the primary LES goes down. The LECS permits two types of backups to be configured: backup LESs that utilize the IBM LES Redundancy VCC as specified in “LAN Emulation Reliability” on page 248, and backup LESs that do not.

The difference between these two options is that in the former option, the LECS attempts to use information on local LESs to determine the correct LES for the client. For example, the LECS can query a local backup LES to determine if the LES is currently in active or in standby mode. In the latter option, the LECS alternately assigns a client to the primary and backup, regardless of any local information. For more information on the redundancy features of the LES, see “LAN Emulation Reliability” on page 248 or the IBM 8210 Multiprotocol Switched Services Server Configuration Program User’s Guide.

You will be prompted to enter the ATM address of the primary and backup LES. If either of the LESs is located on the same MSS Server, then you can select the local option when prompted. Using this option, you do not need to know the 20-byte ATM address of the LES; it will be determined at run-time. If no backup support is provided for a particular LES, select the unspecified option.

For the **les disable**, **les enable**, and **les remove** commands, you are asked to select the LES to which the action applies.

The **les list** command displays the ATM address information for all LESs serving the selected ELAN.

Commands that can be used with the **les** command are illustrated in the following examples:

Syntax:

les	add
	disable
	enable
	list
	remove
	set ...

Example:

```
Selected ELAN 'lgrove01'>les add
  (  1) Local
  (  2) Remote
Primary LES is [1]? 2
If primary LES is remote, enter ATM address
         []? 39.999999999999.000099990101.222222222222.04
  (  1) Unspecified
  (  2) Local
  (  3) Remote
Backup LES is  [1]? 3
If backup LES is remote, enter ATM address
         []? 39.999999999999.000099990102.001bcda02038.07
Do the LESs utilize IBM LES redundancy? [Yes]?: yes
LES ATM address 39.99.99.99.99.99.99.00.00.99.99.01.01.22.22.22.22.2
    added to ELAN 'lgrove01'
```

Example:

```
Selected ELAN 'lgrove01'>les disable
  ATM address of LES for ELAN
   (1) All
   (2) Local LES for: lgrove01

Enter Selection:  [1]?2
LES disabled: Local LES for: lgrove01
Selection "LES disable" Complete
Selected ELAN 'lgrove01'>
```

Example:

```
Selected ELAN 'lgrove01'>les enable
  ATM address of LES for ELAN
   (1) All
   (2) Local LES for: lgrove01

Enter Selection:  [1]?2
LES enabled: Local LES for: lgrove01
Selection "LES ATM address enable" Complete
Selected ELAN 'lgrove01'>
```

Example:

```
Selected ELAN 'lgrove01'>les list
LESs for ELAN 'lgrove01'

Enbld  LES ATM address
=====  ============================================================
Yes  Local LES for: lgrove01
     no backup provided
Selected ELAN 'lgrove01'>
```

Example:

```
Selected ELAN 'lgrove01'>les remove
ATM address of LES for ELAN

 (1) All
 (2) Local LES for: lgrove01
 (3) < CANCEL >
Enter Selection:  [1]?2
Values assigned to LES removed
Delete LES: Local LES for: lgrove01
Selection "LES ATM address removal" Complete
Selected ELAN 'lgrove01'>
```

Use the **les set** command to modify the configuration of a particular LES. Use the **les set primary** command to modify the ATM address of the primary LES, and use the **les set backup** command to modify the ATM address of the backup LES.

Example: les set backup

```
  Selected ELAN 'lgrove01'>les set ba
    (  1) Local LES for: lgrove01
    (  2) 39.99.99.99.99.99.99.00.00.99.99.01.01.22.22.22.22.22.22.04
  Choice of LES [1]? 2
    (  1) Unspecified
    (  2) Local
    (  3) Remote
  Backup LES is  [3]? 3
  If backup LES is remote, enter ATM address
           [39.99.99.99.99.99.99.00.00.99.99.01.02.00.1B.CD.A0.20.38.06]?
  39.99.99.99.99.99.99.00.00.99.99.01.02.00.1B.CD.A0.20.38.06
  Do the LESs utilize IBM LES redundancy?? [Yes]: no
  Backup LES ATM address modified
```

Example: les set primary

```
Selected ELAN 'Accounting Ethernet Elan'> les set primary
  (  1) Local LES for: Accounting Ethernet Elan

Choice of LES [1]?1
```

```
  (  1) Local
  (  2) Remote

Primary LES is [1]?2
If primary LES is remote, enter ATM address
[Local LES for: Accounting Ethernet Elan]?39.00.00.00.00.00.00.d0.d0.d0.d0.d0.d0.10.10.10.10.10.10.03

Primary LES ATM address modified
Selected ELAN 'Accounting Ethernet Elan'>
```

List

The **list** command provides the following information:

Syntax:

list

Example: `list`

```
Selected ELAN 'lgrove01'> list
ELAN Configuration:
ELAN is          Enabled
Name:            'lgrove01'
ELAN Type:       TokenRing
Max Frame Size:  1516
Selected ELAN 'lgrove01'>
```

Policy

Use the **policy** command to add, disable, enable, list, or remove policy values that are assigned to the LESs serving the selected ELAN.

add Use the **policy add** command to add a binding between a policy value and a LES to the static configuration of the LECS. Policy values are used to assign clients to LESs. Refer to “Overview of the LECS Function” on page 238 for details on how the LECS uses policy values to assign LECs to LESs.

Syntax:

policy add pv_type

Where *pv_type* is either:

- ESI/SEL of ATM address
- FRAME size
- MAC address
- NAME of ELAN
- PREFIX of ATM Address
- ROUTE descriptor
- TYPE of Elan

Example:

```
Selected ELAN 'lgrove01'>policy add prefix
 ATM address of LES for policy value(s)

  (1) Local LES for: lgrove01

Enter Selection:  [1]?1
ATM prefix [ ]?55
ATM address prefix 55
bound to LES Local LES for: lgrove01
Configure another address?? [Yes]:no
Selected ELAN 'lgrove01'>
```

Detailed ELAN Configuration

disable

Use the **policy disable** command to disable a policy value in the static configuration of the LECS. This policy value will not become active on the next router restart.

Syntax:

policy disable pv_type

Where *pv_type* is either:

- ESI/SEL of ATM address
- FRAME size
- MAC address
- NAME of ELAN
- PREFIX of ATM address
- ROUTE descriptor
- TYPE of ELAN

Example:

```
Selected ELAN 'lgrove01'>policy disable prefix
ATM prefix
(1) All
(2) 55
LES for: lgrove01
Enter Selection:   [1]? 2
ATM value disabled: 55
Selection "ATM address disable" Complete
Selected ELAN 'lgrove01'>
```

enable

Use the **policy enable** command to enable a policy value in the static configuration of the LECS. The policy value must be enabled to become active at the next router restart.

Syntax:

policy enable pv_type

Where *pv_type* is either:

- ESI/SEL of ATM address
- FRAME size
- MAC address
- NAME of ELAN
- PREFIX of ATM address
- ROUTE descriptor
- TYPE of ELAN

Example:

```
Selected ELAN 'lgrove01'>policy enable prefix
ATM prefix
 (1) All
 (2) 25                                  to Local LES for: lgrove01
 (3) 55                                  to Local LES for: lgrove01

Enter Selection:  [1]?1
Enabled all ATM prefixes for ELAN 'lgrove01'
Selection "ATM address enable" Complete
Selected ELAN 'lgrove01'>
```

list

Use the **policy list** command to display all of the policy values assigned to LESs of the selected ELAN.

Syntax:

policy list pv_type

Where *pv_type* is either:

- all
- ESI/SEL of ATM address
- FRAME size
- MAC address
- NAME of ELAN
- PREFIX of ATM address
- ROUTE descriptor
- TYPE of ELAN

Example:

```
Selected ELAN 'lgrove01'>policy list prefix
ATM prefixes for ELAN 'lgrove01'
Enabled  Value  =>  LES
=======  ========================================
 Yes     55
  => Local LES for: lgrove01
 Yes     25
  => Local LES for: lgrove01

Selected ELAN 'lgrove01'>
```

remove

Use the **policy remove** command to remove policy values from the static configuration of the LECS. You will be prompted to select the policy value to remove.

Syntax:

policy rremove pv_type

Where *pv_type* is either:

- ESI/SEL of ATM address
- FRAME size
- MAC address
- NAME of ELAN
- PREFIX of ATM address
- ROUTE descriptor
- TYPE of ELAN

Example:

```
Selected ELAN 'lgrove01'>policy remove prefix
 ATM prefix
  (1) All
  (2) 55          to Local LES for: lgrove01
LES for: lgrove01

Enter Selection:   [1]? 2
ATM addr prefix deleted: 55
Selection "ATM address removal" Complete
Selected ELAN 'lgrove01'>
```

Set

Use the **set** command to modify the configuration of the selected ELAN. You can enable or disable the ELAN, or modify its name, type, or maximum frame size. Parameters that you can use with the **set** command are illustrated in the following examples:

Syntax:

set enable-disable
frame
name
type

Example:

```
Selected ELAN 'lgrove01'>set enable-disable
Enable ELAN for LEC assignment [yes]yes
ELAN enable-disable modified
Selection "ELAN enable-disable modification" Complete
Selected ELAN 'lgrove01'>
```

Example:

```
Selected ELAN 'lgrove01'>set frame
Maximum frame size of ELAN
 (1) 1516
 (2) 4544
 (3) 9234
 (4) 18190
 (5) 1580
Enter Selection:  [2]?2
ELAN max frame size modified
Selection "ELAN max frame size modification" Complete
Selected ELAN 'lgrove01'>
```

Example:

```
Selected ELAN 'lgrove01'> set name
Name of ELAN [lgrove01]lgrove001
ELAN name changed to 'lgrove001'
Selection "ELAN name modification" Complete
Selected ELAN 'lgrove001'>
```

Example:

```
Selected ELAN 'lgrove01'>set type
Type of ELAN
 (1) Ethernet
 (2) TokenRing

Enter Selection:  [2]?2
ELAN type modified
Selection "ELAN type modification" Complete
Selected ELAN 'lgrove001'>
```

ELAN-TLV

Type/length/values (TLVs) are optional configuration parameters that can be returned to all clients assigned to the selected ELAN. ELAN-TLVs are TLVs that should be returned to all clients assigned to the selected ELAN.

See “LEC-TLV” on page 394 for information about configuring TLVs that are returned to a particular LEC assigned to the selected ELAN.

Table 53. Selected ELAN-TLV Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds a TLV to the selected ELAN.
Disable	Disables a TLV for the selected ELAN.
Enable	Enables a TLV for the selected ELAN.
List	List the configured ELAN-TLVs.
Remove	Removes a TLV from the selected ELAN.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Use the **elan-tlv add** command to add the specified TLVs of the selected ELAN. You can use the following parameters with the **elan-tlv** command:

- ATM Forum TLVs
- IBM TLVs
- MPS (MPOA Server) TLVs
- MPC (MPOA Client) TLVs
- User Defined TLVs

elan-tlv add

Syntax:

elan-tlv add atm

Choose from :

- C7 : Control timeout
- C10:Maximum unknown frame count
- C11:Maximum unknown frame time
- C12:VCC timeout period
- C13:Maximum retry count
- C17:Aging time
- C18:Forward delay time
- C20:Expected LE_ARP response time
- C21:Flush timeout
- C22:Path switching delay
- C23:Local segment ID
- C24:Mcast send VCC type
- C25:Mcast send VCC avg rate
- C26:Mcast send VCC peak rate
- C28:Connection complete timer
- C31: ELAN Identifier
- C35: Preferred LES

Syntax:

elan-tlv add ibm

Choose from :

- I4: Validate PCR of DDVCCs
- I5: Maximum Reserved Bandwidth of DDVCCs
- I6: Requested DDVCC Type
- I7: Requested DDVCC Peak Cell Rate
- I8: Requested DDVCC Avg Cell Rate
- I9: Requested DDVCC QoS Class
- I10: Negotiate Cell Rates on DDVCCs
- I11: Maximum burst size of DDVCCs

Syntax:

elan-tlv add mps

Choose from :

- p1: Keep-Alive Time
- p2: Keep-Alive Lifetime
- p3: InternetWork-layer Protocols
- p4: Initial Retry Time
- p5: Retry Time Maximum
- p6: Give-up Time
- p7: Hold Down Time

Syntax:

elan-tlv add mpc

Choose from :

- p1: SC-Setup Frame Count
- p2: SC-Setup Frame Time
- p3: Flow-detection Protocols
- p4: Initial Retry Time
- p5: Retry Time Maximum
- p6: Hold Down Time

Syntax:

elan-tlv add user

You can define and add their own TLVs.

Example:

```
Selected ELAN 'joe'> elan-tlvs add user
Type of TLV (in hex) [0]
Description of TLV user-tlv example
Length of TLV [4]
Value of TLV (in hex) [] cabacaba
TLV added: user-tlv example
Selection "Flush timeout TLV add" Complete
Selected ELAN 'joe'>
```

disable

Use the **elan-tlv disable** command to disable a TLV in the static configuration. The TLV will not become active on the next router restart. You are prompted to select the TLV to disable.

Syntax:

elan-tlv disable

Example:

```
Selected ELAN 'lgrove001'> elan-tlv disable
TLV choice:
        (1) All
        (2) T x00A03E01 C7 : Control timeout (sec)       L 2   V 120
        (3) T x00A03E02 C10: Maxmm unknown frame count   L 2   V 1
        (4) T x00A03E03 C11: Mxmm unknwn frm time (sec)  L 2   V 1
        (5) T x00A03E04 C12: VCC timeout period (sec)    L 4   V 1200
        (6) T x00A03E05 C13: Maximum retry count         L 2   V 1
        (7) T x00A03E06 C17: Aging time (sec)            L 4   V 300
        (8) T x00A03E07 C18: Forward delay time (sec)    L 2   V 15
        (9) T x00A03E08 C20: Expctd LE_ARP rspnse (sec)  L 2   V 1
        (10) T x00A03E09 C21: Flush timeout (sec)         L 2   V 4
        (11) T x00A03E0A C22: Path switching delay (sec)  L 2   V 6
        (12) T x00A03E0B C23: Local segment ID (hex)      L 2   V ff:00
        (13) T x00A03E0C C24: Mcst send VCC type (dec)    L 2   V 2
        (14) T x00A03E0D C25: Mcst snd VCC avrg rt (cps)  L 4   V 0
        (15) T x00A03E0E C26: Mcst snd VCC peak rt (cps)  L 4   V 0
        (16) T x00A03E0F C28: Cnnctn complete time (sec)  L 2   V 4

 Enter Selection:  [1]? 1
 Disabled all TLVs for ELAN 'lgrove001'
 Selection "TLV disable" Complete
 Selected ELAN 'lgrove001'>
```

enable

Use the **elan-tlv enable** command to enable a TLV in the static configuration. The selected TLV will become active on the next router restart. You are prompted to select the TLV to enable.

Syntax:

elan-tlv enable

```
selected ELAN 'lgrove001'> elan-tlv enable
TLV choice:
        (1) All
        (2) T x00A03E01 C7 : Control timeout (sec)       L 2   V 120
        (3) T x00A03E02 C10: Maxmm unknown frame count   L 2   V 1
        (4) T x00A03E03 C11: Mxmm unknwn frm time (sec)  L 2   V 1
        (5) T x00A03E04 C12: VCC timeout period (sec)    L 4   V 1200
        (6) T x00A03E05 C13: Maximum retry count         L 2   V 1
        (7) T x00A03E06 C17: Aging time (sec)            L 4   V 300
        (8) T x00A03E07 C18: Forward delay time (sec)    L 2   V 15
        (9) T x00A03E08 C20: Expctd LE_ARP rspnse (sec)  L 2   V 1
        (10) T x00A03E09 C21: Flush timeout (sec)         L 2   V 4
        (11) T x00A03E0A C22: Path switching delay (sec)  L 2   V 6
        (12) T x00A03E0B C23: Local segment ID (hex)      L 2   V ff:00
        (13) T x00A03E0C C24: Mcst send VCC type (dec)    L 2   V 2
        (14) T x00A03E0D C25: Mcst snd VCC avrg rt (cps)  L 4   V 0
        (15) T x00A03E0E C26: Mcst snd VCC peak rt (cps)  L 4   V 0
        (16) T x00A03E0F C28: Cnnctn complete time (sec)  L 2   V 4
Enter Selection:  [1]?1
Enabled all TLVs for ELAN 'lgrove001'
Selection "TLV enable" Complete
Selected ELAN 'lgrove001'>
```

list Use the **elan-tlv list** command to list all TLVs of the selected ELAN.

Syntax:

elan-tlv list

```
Selected ELAN 'lgrove001'> elan-tlv list
            TLVs for ELAN 'lgrove001'

 Enabled  TLV
 =======  ========================================================
     Yes  Type: x00A03E01 'C7 : Control timeout (sec)'
          Len: 2 Value: 120
     Yes  Type: x00A03E02 'C10: Maxmm unknown frame count'
          Len: 2 Value: 1
     Yes  Type: x00A03E03 'C11: Mxmm unknwn frm time (sec)'
          Len: 2 Value: 1
     Yes  Type: x00A03E04 'C12: VCC timeout period (sec)'
          Len: 4 Value: 1200
     Yes  Type: x00A03E05 'C13: Maximum retry count'
```

```
     Len: 2 Value: 1
Yes  Type: x00A03E06 'C17: Aging time (sec)'
     Len: 4 Value: 300
Yes  Type: x00A03E07 'C18: Forward delay time (sec)'
     Len: 2 Value: 15
Yes  Type: x00A03E08 'C20: Expctd LE_ARP rspnse (sec)'
     Len: 2 Value: 1
Yes  Type: x00A03E09 'C21: Flush timeout (sec)'
     Len: 2 Value: 4
Yes  Type: x00A03E0A 'C22: Path switching delay (sec)'
     Len: 2 Value: 6
Yes  Type: x00A03E0B 'C23: Local segment ID (hex)'
     Len: 2 Value: ff:00
Yes  Type: x00A03E0C 'C24: Mcst send VCC type (dec)'
     Len: 2 Value: 2
Yes  Type: x00A03E0D 'C25: Mcst snd VCC avrg rt (cps)'
     Len: 4 Value: 0
Yes  Type: x00A03E0E 'C26: Mcst snd VCC peak rt (cps)'
     Len: 4 Value: 0
Yes  Type: x00A03E0F 'C28: Cnnctn complete time (sec)'
     Len: 2 Value: 4

Selected ELAN 'lgrove001'>
```

remove

Use the **elan-tlv remove** command to remove a TLV from the static configuration of the selected ELAN. You are prompted to select the TLV to remove.

Syntax:

elan-tlv remove

Example:

```
Selected ELAN 'lgrove001'> elan-tlv remove
TLV Choice:
        (1) All
        (2) T x00A03E01 C7 : Control timeout (sec)       L 2   V 120
        (3) T x00A03E02 C10: Maxmm unknown frame count   L 2   V 1
        (4) T x00A03E03 C11: Mxmm unknwn frm time (sec)  L 2   V 1
        (5) T x00A03E04 C12: VCC timeout period (sec)    L 4   V 1200
        (6) T x00A03E05 C13: Maximum retry count         L 2   V 1
        (7) T x00A03E06 C17: Aging time (sec)            L 4   V 300
        (8) T x00A03E07 C18: Forward delay time (sec)    L 2   V 15
        (9) T x00A03E08 C20: Expctd LE_ARP rspnse (sec)  L 2   V 1
        (10) T x00A03E09 C21: Flush timeout (sec)        L 2   V 4
        (11) T x00A03E0A C22: Path switching delay (sec) L 2   V 6
        (12) T x00A03E0B C23: Local segment ID (hex)     L 2   V ff:00
        (13) T x00A03E0C C24: Mcst send VCC type (dec)   L 2   V 2
        (14) T x00A03E0D C25: Mcst snd VCC avrg rt (cps) L 4   V 0
        (15) T x00A03E0E C26: Mcst snd VCC peak rt (cps) L 4   V 0
        (16) T x00A03E0F C28: Cnnctn complete time (sec) L 2   V 4

Enter Selection:  [1]?2

           TLV deleted: T x00A03E01 C7 : Control timeout (sec)       L 2   V 120
           Selection "TLV remove" Complete
           Selected ELAN 'lgrove001'>
```

LEC-TLV

Type/length/values (TLVs) can be associated with an individual LEC or group of LECs assigned to the selected ELAN. The LECs can be identified by any of the following policy values:

- ATM address
- MAC address
- Route descriptor
- ELAN name

Note: These policies must be already configured on this ELAN with the **policy add** command.

For example, LEC-TLVs can be used to distinguish LECs with different QoS, giving their traffic different priority or bandwidth than other LECs associated with the same ELAN.

See “ELAN-TLV” on page 390 for information about configuring TLVs to be associated with all LECs assigned to the selected ELAN.

The following table shows the different identifiers you can use to select the individual LECs associated with a particular policy.

Table 54. Selected LEC-TLV Identifiers Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
ESI/SEL of ATM address	Uses an ESI/Selector of ATM address policy to identify the LECs to be associated with the TLV.
MAC address	Uses a MAC address policy to identify the LECs to be associated with the TLV.
Name of ELAN	Uses an ELAN name policy to identify the LECs to be associated with the TLV.
PREFIX of ATM address	Uses an ATM address prefix policy to identify the LECs to be associated with the TLV.
Route Descriptor	Uses a route descriptor policy to identify the LECs to be associated with the TLV.

After a policy is chosen, you can use the following commands to configure detailed TLVs to be returned to all LECs assigned by the selected policy.

Table 55. Selected LEC-TLV Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds a TLV to the selected ELAN policy.
Disable	Disables a TLV for the selected ELAN policy.
Enable	Enables a TLV for the selected ELAN policy.
List	Lists TLVs for the selected ELAN policy.
Remove	Removes a TLV from the selected policy.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Example:

```
 Selected ELAN 'lgrove01'>policy list prefix

ATM prefixes for ELAN 'lgrove01'
Enabled  Value  =>  LES
=======  ========================================
     No  55
            => Local LES for: lgrove01
     No  25
            => Local LES for: lgrove01
Selected ELAN 'lgrove01'>lec-tlv prefix
  (  1) 55
  (  2) 25
ATM prefix [1]?
Policy Value '55' selected for detailed TLV configuration
Tlvs for '55' selected>add ibm i4
I4: Validate peak cell rate of Best Effort DDVCCs? [No]: yes
TLV added: I4: Vldt PCR of Bst Effrt DDVCC
```

Detailed ELAN Configuration

```
Tlvs for '55' selected>list
Enabled  TLV
=======  ======================================================
    Yes  Type: x10005A04 'I4: Vldt PCR of Bst Effrt DDVCC'
         Len: 4 Value: 1

Tlvs for '55' selected>
```

Configuration Commands for the Policies of a LECS

This section describes the commands to modify the policies that guide the LECS-to-LES assignment procedure. Enter the **policies** command at the `LECS config>` prompt to get to the `LECS Policies config>` prompt where you can enter the following commands:

Table 56. LECS Policies Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Add a policy to the static configuration of the LECS.
Disable	Disable a policy of the LECS.
Enable	Enable a policy of the LECS.
List	Lists policies configured for LECS.
Remove	Remove a policy of the LECS.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

The **add** command adds a policy to the LECS. When adding a policy, you are prompted for the “priority” and “type” of the policy.

Priority specifies the order in which policies are considered; policies with lower priorities are considered earlier. For a more detailed explanation of policies and how the LECS is guided by them, refer to “Overview of the LECS Function” on page 238.

Type specifies what information about the client should be used to assign it at the specified priority.

Syntax:

add

Example:

```
LECS Policies config> add
Priority of Policy [10]?10
Policy type
 (1) byAtmAddr
 (2) byMacAddr
 (3) byRteDesc
 (4) byLanType
 (5) byPktSize
 (6) byElanNm

Enter Selection: [1]?1
Added policy 'byAtmAddr' at priority 10
Selection "Add assignment policy" Complete
LECS Policies config>
```

Disable

The **disable** command disables a policy in the static configuration of the LECS. Disabled policies will not become active on the next router restart.

Syntax:

disable

Example:

```
LECS Policies config> disable
Choice of policy
 (1) All
 (2) 10 byAtmAddr

Enter Selection: [1]?1
Disabled all policies
Selection "Disable assignment policy" Complete
LECS Policies config>
```

Enable

The **enable** command enables a policy in the static configuration of the LECS. Enable policies become active on the next router restart.

Syntax:

enable

enable

Example:

```
LECS Policies config> enable
Choice of policy
 (1) All
 (2) 10   byAtmAddr
Enter Selection:  [1]?2
Enabled policy '10   byAtmAddr'
Selection "Enable assignment policy" Complete
LECS Policies config>
```

List

The **list** command lists the policies currently configured for the LECS.

Syntax:

list

Example:

```
LECS Policies config> list
Policy Listing...
Enabled  Priority  Type
=======  ========  ===========
    Yes        10  byAtmAddr
LECS Policies config>
```

Remove

The **remove** command removes a policy from the static configuration of the LECS.

Syntax:

Configuring the Policies of a LECS

remove

Example:

```
LECS Policies config> remove
Choice of policy
 (1) All
 (2) 10 byAtmAddr
Enter Selection: [1]?1
Removed all policies
Selection "Remove assignment policy" Complete
LECS Policies config>
```

Configuration Commands for Security for ELANs

This section describes optional commands related to authentication of LE Client requests to join ELANs. The LES-LECS Security Interface is the LE Services component responsible for multiplexing configuration requests from the LESs on the MSS Server to the LECS (which may or may not be on the MSS Server). The LES-LECS interface is a required component if any of the LES-BUSs are using the security features of the MSS Server. See “LAN Emulation Security” on page 250 for additional information.

Enter the **security** command at the `LE-Services config>` prompt to get to the `LECS INTERFACE config>` prompt.

Table 57. LECS Interface Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Provides for authentication of client-joins.
Disable	Disables ability to authenticate client-joins.
Enable	Enables ability to authenticate client-joins.
List	Lists parameters for this interface.
Remove	Removes ability to authenticate client-joins.
Set	Sets parameters for this interface (ATM address and traffic type).
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to add a communication path to the LECS authentication of client-joins.

Syntax:

add

Example:

```
LECS INTERFACE config> add
  (  1) Use burned in ESI
Select ESI [1]?1
Selector 0 is generally reserved for use by the LECS,
Selector 1 is generally reserved for use by the LECS Interface.
LECS Interface Selector [1]?1
LECS INTERFACE config>
```

Disable

Use the **disable** command to disable LECS authentication of client-joins.

Syntax:

disable

Example: `disable`

Enable

Use the **enable** command to enable LECS authentication of client-joins.

Syntax:

enable

Example: `enable`

List

Use the **list** command to see a detailed list of the parameters associated with this LECS interface.

Syntax:

list

Example:

```
LECS INTERFACE config> list
LECS Interface Detailed Configuration
   LECS Interface Enabled/Disabled: Enabled
   ATM Device number: 0
   ESI: Use Burned in ESI
   Selector: 0x01
   Configuration Direct VCC Traffic Type: Best Effort VCC
   Configuration Direct VCC PCR in Kbps: 155000
   Configuration Direct VCC SCR in Kbps: 0
LECS INTERFACE config>
```

Remove

Use the **remove** command to remove the ability to authenticate client-joins for this ELAN.

Syntax:

remove

Example: `remove`

Set

Use the **set** command to configure the address and the traffic type for this interface.

Syntax:

set address

traffic

Example:

```
LECS INTERFACE config> set address
  (  1) Use burned in ESI
Select ESI [1]?
Selector 0 is generally reserved for use by the LECS,
Selector 1 is generally reserved for use by the LECS Interface.
LECS Interface Selector [1]?1
LECS INTERFACE config>
```

Example:

```
LECS INTERFACE config> set traffic configuration
  (  1) Best Effort
  (  2) Reserved Bandwidth
Traffic type [1]?1
Peak cell rate in Kbps (1-155000) [155000]? 75000
LECS INTERFACE config>
```

Accessing the LAN Emulation Services Monitoring Environment

The LE Services monitoring environment (available from the GWCON process) is characterized by the LE-SERVICES+ prompt. Commands entered at this prompt permit you to work more closely with a particular LE component, or to create a LES-BUS.

To access the LE Services console:

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, refer to "What is the OPCON Process?" on page 75.) For example:

   ```
   * talk 5
   +
   ```

   The GWCON prompt (+) is displayed on the console. If the prompt does not appear when you first enter GWCON, press **Return** again.

2. At the GWCON prompt, enter the **network** command to display the network interface numbers for which the router is currently configured. For example:

   ```
   *talk 5
   +network ?
   0  : ATM
   Network number [0]? 0
   ATM Console
   ATM+
   ```

   Note: Depending on your hardware, two ATM interfaces may be defined.

3. Enter the **le-services** command

   Example:

   ```
   ATM+le-s
   LE-Services Console
   LE-SERVICES+
   ```

Monitoring Commands for LAN Emulation Services

Enter commands at the LE-Services+ prompt.

Table 58. LAN EMULATION Services Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.

Table 58. LAN EMULATION Services Monitoring Commands Summary (continued)

Command	Function
Create	Creates an operating LES-BUS from its configuration data (the configuration data must also exist).
Lecs	Takes you to the LECS monitoring environment, described in "Monitoring Commands for LECS" on page 442.
Les-bus	Takes you to the monitoring environment for a particular LES-BUS, as described in "Monitoring Commands for LES-BUS" on page 404.
List	Displays a list of the operating LES-BUSs.
Security	Takes you to the LES-LECS Security monitoring environment, described in "Monitoring Commands for Security for LE Service" on page 469.
Summary	Displays a summary of the operating LES-BUSs, including the number of operational LE Clients.
Work	Takes you to the monitoring environment for a particular LES-BUS, as described in "Monitoring Commands for LES-BUS" on page 404.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

Create

Use the **create** command to create an operating LES-BUS from its configuration. Before you can create a LES-BUS, its configuration must first exist. See "Configuration Commands for a LES-BUS" on page 354 for an explanation of how to configure a LES-BUS.

Syntax:

create *elan-name*

where *elan-name* is the name of the ELAN.

Example:

```
LE-SERVICES+ create
ELAN Name (ELANxx) []? IBM Token Ring Test ELAN!
LES/BUS: 'IBM Token Ring Test ELAN!': STARTING
```

Lecs

Use the **lecs** command to enter the LECS monitoring environment.

Syntax:

lecs

Example:

```
LE-SERVICES+ lecs
LECS console+
```

Les-bus

Use the **les-bus** command to enter the monitoring environment for a particular operating LES-BUS. A selection list will appear, or one can use the **list** or **summary** command to display all of the operating LES-BUSs.

Syntax:

LE Services monitoring commands

les-bus *elan-name*

item-number

elan-name
Name of the ELAN.

item-number
Item number from selection list.

Example: `les-bus`

```
LE-SERVICES+ les
  (  1) boston
  (  2) chicago
  (  3) losangeles
  (  4) miami
  (  5) newyork

Choice of LES/BUS [1]? 3
LE-Services Console for an existing LES-BUS Pair
EXISTING LES-BUS 'losangeles'
```

Example: `les-bus` *elan-name*

```
LE-SERVICES+ les losangeles
LE-Services Console for an existing LES-BUS Pair
EXISTING LES-BUS 'losangeles'+
```

Example: `les-bus` *item-number*

```
LE-SERVICES+ les 3
LE-Services Console for an existing LES-BUS Pair
EXISTING LES-BUS 'losangeles'+
```

List

Use the **list** command to display a list of the currently operating LES-BUSs and their ATM addresses. Use the **summary** command to display the number of operational LE clients.

Syntax:

list

Example:

```
LE-SERVICES+list
ELAN Type  (E=Ethernet/802.3, T=Token Ring/802.5)
| Interface #
| |  LES-BUS State  (UP=Up,  RE=Redun.  ID=Idle,  ND=Net Down,  ER=Error/Down,
| | |                **=Other; Work with specific LES-BUS to see actual state)
| | |
| | | ELAN Name                       LES ATM Addr
- - -- ------------------------------ ----------------------------------------
E 0 RE e1                            39999999999999000099990200000 4AC47391803
T 0 UP t1                            39999999999999000099990200000 4AC47391802
LE-SERVICES+
```

Security

Use the **security** command to enter the monitoring environment for the LES-LECS Security Interface component. This is the component that multiplexes security requests between the LE Servers on this router and the LECS (which may or may not be on this router).

Syntax:

security

Example:

```
LE-SERVICES+ security
LES-LECS Security Interface
LES-LECS interface+
```

Summary

Use the **summary** command to display a summary of the currently operating LES-BUSs including the number of operational LE Clients.

Syntax:

summary

Example:

```
LE-SERVICES+ summary

ELAN Type  (E=Ethernet/802.3, T=Token Ring/802.5)
| Interface #
| |  LES-BUS State  (UP=Up,  RE=Redun.  ID=Idle,  ND=Net Down,  ER=Error/Down,
| |  |               **=Other; Work with specific LES-BUS to see actual state)
| |  |
| |  |                                                          Last LES/BUS
| |  |                                        #LECs      #LECs   State Change
| |  | ELAN Name                              Proxy   NonProxy   (Sys uptime)
- - -- -------------------------------  ------   --------   ------------
E 0 RE e1                                    (Redundant)    00.08.53.30
T 0 UP t1                                 0          2    00.13.07.77
LE-SERVICES+
```

Work

Use the **work** command to enter the monitoring environment for a particular operating LES-BUS. A selection list will appear or you can use the **list** command or **summary** command to display all of the operating LES-BUSs.

Syntax:

work *elan-name*

item-number

elan-name
Name of the ELAN.

item-number
Item number from selection list.

Example: work

```
LE-SERVICES+ work
  (  1) boston
  (  2) chicago
  (  3) losangeles
  (  4) newyork
  (  5) miami
 Choice of LES/BUS [1]? 3
LE-Services Console for an existing LES-BUS Pair
EXISTING LES-BUS 'losangeles'+
```

Example: work *elan-name*

```
LE-SERVICES+ work losangeles
LE-Services Console for an existing LES-BUS Pair
EXISTING LES-BUS 'losangeles'+
```

Example: work *item-number*

```
LE-SERVICES+ work 3
LE-Services Console for an existing LES-BUS Pair
EXISTING LES-BUS 'losangeles'+
```

Monitoring Commands for LES-BUS

Enter commands at the `EXISTING LES-BUS+` prompt.

Table 59. LES-BUS Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Bus-filter	Accesses the Bus filter console.
Bus-police	Accesses the Bus police console.
Database	Flushes all cache entries for a specified Broadcast Manager Protocol, or lists database entries.
Delete	Deletes a LES-BUS.
Disable	Disables an existing LES-BUS component: Broadcast Manager (IP, IPX, IPX Server Farm Detection, or NetBIOS), BUS Monitor, Redundancy, Security, Bus Filter, Bus Police, or Source Route Manager. It disables the chosen option immediately, but the LES-BUS’s configured state in Static RAM does not change.
Enable	Enables an existing LES-BUS component: Broadcast Manager (IP, IPX, IPX Server Farm Detection, or NetBIOS), BUS Monitor, Redundancy, Security, Bus Filter, Bus Police, or Source Route Manager. It enables the chosen option immediately, but the LES-BUS’s configured state in Static RAM does not change.
List	Lists the status and current configuration parameters of the LES-BUS.
Remove	Removes a bus-filter item from the bus filter or removes a device from the immunity list or filter list of the BUS Police function.
Restart	Restarts a running or stopped LES-BUS. A LES-BUS can be restarted using the parameters configured under the Talk 5 or Talk 6 interface.
Set	Sets LES-BUS configuration parameters. The parameter that you set is immediately used by the LES-BUS, but the LES-BUS’s configured parameter values in Static RAM do not change.
Show	Shows information on LES-BUS databases, statistics, VCCs, Bus Filter filter-items, Bus Police immunity lists, or current configuration.
Statistics	Clears or displays LES-BUS statistics.
Stop	Stops the operation of LES-BUS.
Takeover	Takes over from an active backup LES-BUS when using LES-BUS Peer Redundancy.
Terminate	Terminates a specified LEC from the LES-BUS.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Bus-filter

Use the **bus-filter** command to access the `BUS FILTER for EXISTING LES-BUS 'x'+` monitoring command prompt from which you can monitor data packet filtering using the following commands:

Table 60. BUS Filter Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds a bus filter item to a local configuration.
Disable	Disables a Bus filter item.
Enable	Enables a Bus filter item.
Remove	Removes a Bus filter item.
Reset	Resets Bus filter counters.
Set	Sets Bus filter parameters.
Show	Displays filter items.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to add data packet filtering.

Syntax:

add ip *filteritem*

mac *address filteritem*

protocol *filteritem*

sliding-window *filteritem*

ip *filteritem*

Adds the specified IP filter item. The following questions will be asked:

IP address type

Specifies whether this IP filter operates on the destination IP address or source IP address. The address is found in the IP header of the packer.

Valid Values: source IP address, destination IP address

Default Value: destination IP address

IP subnet

Identifies the subnet or IP address that is to be filtered.

Valid Values: 0.0.0.0 - 255.255.255.255

Default Value: 0.0.0.0

IP subnet mask

Identifies the IP mask used to determine the subnet or IP address of the data packet.

Valid Values: 0.0.0.0 - 255.255.255.255

Default Value: 0.0.0.0

Filter list

Identifies the filter list for which this filter definition is configured.

Valid Values: EXCLUDE, INCLUDE

Default Value: EXCLUDE

Enable this filter?

Identifies whether the filter is to be enabled or disabled.

Valid Values: yes, no

Default Value: yes

Enter filter name
Specifies a name to be associated with this filter.

Valid Values: Any character string up to 32 characters in length

Default Value: None

MAC *address filteritem*
Adds the specified MAC filter item at the specified MAC address. The following questions will be asked:

Mac address type
Specifies whether this filter operates on the destination MAC address or source MAC address.

Valid Values: source MAC address, destination MAC address

Default Value: source MAC address

MAC address
Identifies the MAC address to be ANDed with the data packet's MAC address mask to generate a data packet MAC filter value.

Valid Values: Any valid MAC address

Default Value: FF.FF.FF.FF.FF.FF

MAC address mask
Identifies the MAC address mask to be ANDed with the data packet's MAC address to generate a data packet MAC filter value.

Valid Values: Any valid MAC address

Default Value: FF.FF.FF.FF.FF.FF

Filter list
Identifies the filter list for which this filter definition is configured.

Valid Values: EXCLUDE, INCLUDE

Default Value: EXCLUDE

Enable this filter?
Identifies whether the filter is to be enabled or disabled.

Valid Values: yes, no

Default Value: yes

Enter filter name
Specifies a name to be associated with this filter.

Valid Values: Any character string up to 32 characters in length

Default Value: None

protocol *filteritem*
Adds the specified protocol filter item. The following questions will be asked:

Protocol
Identifies the protocol type to be managed for BUS filter.

Valid Values:

- IP

- IPX
- NetBIOS
- AppleTalk
- Banyan Vines
- NetBIOS over IP
- IP multicast
- IPX type 20
- BPDU

Default Value: IP

Filter list
Identifies the filter list for which this filter definition is configured.

Valid Values: EXCLUDE, INCLUDE

Default Value: EXCLUDE

Enable this filter?
Identifies whether the filter is to be enabled or disabled.

Valid Values: yes, no

Default Value: yes

Enter filter name
Specifies a name to be associated with this filter.

Valid Values: Any character string up to 32 characters in length

Default Value: None

sliding—window *filteritem*
Adds the specified sliding window filter item. When using Token Ring, the information field is the byte following the RIF field. When using Ethernet, the information field is the information following the length field or the Ethertype (802.3) field. The following questions will be asked:

Filter base
Identifies the

Valid Values: mac, info

Default Value: info

Window filter offset
Identifies the packet offset to begin the sliding window test.

Valid Values: 0 - 255

Default Value: 0

Compare value
Specifies the compare value for the sliding window filter. Sliding window data compared with the packet data starting at the specified offset in the packet.

Valid Values: 1 - 32 hexadecimal bytes

Default Value: none

Compare mask
Specifies the compare mask for the sliding window filter. The sliding window mask ANDed with the packet data starting at the offset in the packet.

Valid Values: 1 - 32 hexadecimal bytes

Default Value: The samenumber of X'F' that are specified in the **Compare value**.

Filter list
Identifies the filter list for which this filter definition is configured.

Valid Values: EXCLUDE, INCLUDE

Default Value: EXCLUDE

Enable this filter?
Identifies whether the filter is to be enabled or disabled.

Valid Values: yes, no

Default Value: yes

Enter filter name
Specifies a name to be associated with this filter.

Valid Values: Any character string up to 32 characters in length

Default Value: None

Disable

Use the **disable** command to disable data packet filtering. Choose the filter item to be disabled from the provided list.

Syntax:

disable ip *filteritem*
mac *address filteritem*
protocol *filteritem*
sliding-window *filteritem*

ip *filteritem*
Disables the specified IP filter item.

MAC *address filteritem*
Disables the specified MAC filter item.

protocol *filteritem*
Disables the specified protocol filter item.

sliding—window *filteritem*
Disables the specified sliding window filter item.

Enable

Use the **enable** command to enable data packet filtering. This lets the BUS use the configured filters to limit data traffic propagated across the ELAN, improving security from unwanted broadcast attacks, improving bandwidth utilization by limiting data traffic, and centralizing filter controls in a single location to facilitate filtering management.

Choose the filter item to be enabled from the provided list.

Syntax:

enable ip *filteritem*
mac *address filteritem*
protocol *filteritem*
sliding-window *filteritem*

ip *filteritem*
Enables the specified IP filter item.

MAC *address filteritem*
Enables the specified MAC filter item.

protocol *filteritem*
Enables the specified protocol filter item.

sliding—window *filteritem*
Enables the specified sliding window filter item.

Remove

Use the **remove** command to remove the specified bus filter for this LES-BUS. Choose the filter item to be removed from the provided list.

Syntax:

remove all
ip *filteritem*
mac *address filteritem*
protocol *filteritem*
sliding-window *filteritem*

all Removes all defined BUS filters.

ip *filteritem*
Removes the specified IP filter item. You will be provided a list of options.

MAC *address filteritem*
Removes the specified MAC filter item at the specified MAC address. You will be provided a list of options.

protocol *filteritem*
Removes the specified protocol filter item. You will be provided a list of options.

sliding—window *filteritem*
Removes the specified sliding window filter item. You will be provided a list of options.

Reset

Use the **reset** command to reset the Bus filter counters.

Syntax:

reset *filter counters*

Set

Use the **set** command to set bus filtering for this LES-BUS.

Syntax:

set default *action*

preferred *list*

default action
Specifies the default action for the Bus filter. This is the action taken if no matches occur on any of the defined filter items.

Valid Values: Exclude, Include

Default Value: Exclude

preferred list
Sets the list that will be evaluated first (exclude or include).

Valid Values: Exclude, Include

Default Value: Exclude

Show

Use the **show** command to display configured Bus filter items.

Syntax:

show

Example:

```
BUS FILTER config for ELAN 'elan01'> show
Bus Filter Items

Default Action:     EXCLUDE
Preferred List:     EXCLUDE LIST
      Enabled?:     NO

MAC Filter Items:

(1)Name:mac01
    Address Type: DESTINATION  List: EXCLUDE LIST  Enabled: YES  Hits:0
    Mac Address: 12.34.56.78.90.12
           Mask: FF.FF.FF.FF.FF.FF

 PROTOCOL Filter Items:

(1)Name:protocol01
    Protocol: BPDU              List: EXCLUDE LIST  Enabled: YES  Hits:0

 SLIDING WINDOW Filter Items:

(1)Name:slide01
    Base: MAC   Offset:   0   List: EXCLUDE LIST   Enabled: YES  Hits:0
    Value: 20
     Mask: F0

 IP Filter Items:

(1)Name:ipfilt01
    Address Type: SOURCE       List: EXCLUDE LIST  Enabled: YES  Hits:0
    Address or Subnet: 0.0.0.0
          Subnet Mask: 0.0.0.0
LES-BUS config for ELAN 'elan01'>
```

Bus-police

Use the **bus-police** command to access the `BUS POLICE for EXISTING LES-BUS 'x'+` monitoring command from which you can use the following commands to provide dynamic traffic management for the BUS:

Table 61. BUS Police Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds a bus police immunity list to a local configuration.
Flush	Flushes all devices from the Bus police immunity list or from the Bus filter filter list.
Remove	Removes an entry from the bus police immunity list or from a filter list
Set	Sets bus police parameters.
Show	Displays bus police immunity list items and bus filter filter list items.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to add a bus police immunity list.

Syntax:

add

Source address

Specifies the source MAC address to be granted immunity.

Valid Values: Any valid MAC address

Default Value: X'00.00.00.00.00.00'

Flush

Use the **flush** command to flush all devices from the BUS Police immunity list or the Bus Police filter list.

Syntax:

flush	**i**mmunity list
	filter list

Remove

Use the **remove** command to remove a MAC address from the immunity list or filter list.

Syntax:

remove	immunity
	filter

You will be provided a list from which to choose the MAC address to be removed.

Set

Use the **set** command to set bus police parameters.

Syntax:

set duration
threshold

Duration of Bus Police management

Specifies the installed BUS Police MAC filter duration:

- Temporary indicates that any MAC filter installed by BUS Police is automatically removed by BUS Police if the offending MAC address's BUS transmit rate falls below the BUS Police **threshold**.
- Permanent indicates that the BUS Police will not remove any installed MAC filters, even if the offending MAC address's BUS transmit rate later falls below the BUS Police threshold. MAC filters installed by the BUS Police when the duration is set to *permanent* can only be removed through manual intervention.

Valid Values: Temporary or Permanent

Default Value: Temporary

Example: `set bus-police duration`

```
Select Bus Police filter duration
         (1) TEMPORARY
         (2) PERMANENT
Enter Selection: [1]
```

threshold in packets per second

Example: `set bus-monitor threshold`

Specifies the BUS Police BUS transmit threshold in packets per second. Packets originating from MAC addresses that exceed this rate during the BUS Moniotr Sample Interval will be filtered.

Valid Values: 1 - 100000

Default Value: 50

```
Enter Bus Police Threshold value (1-100000) [50]?
```

Show

Use the **show** command to display the configured Bus police immunity list.

Syntax:

show

Example:

```
BUS POLICE config for ELAN 'elan01'> show
Bus Police Filter Lists

Threshold:     1
Duration:     PERMANENT
Enabled?:     NO

   Bus Police Immunity List
   Mac Address
```

```
-----------------
12.34.56.78.90.12
22.33.44.55.66.11

Bus Police Filter List
Mac Address              Filter Hits
----------------         -----------
NONE DEFINED
```

Database

The **database** command has two uses. You can use it to **flush** all cache entries for a Broadcast Manager Protocol, or to **list** information about database entries. See “Database Flush” on page 413, “Database List” on page 413, and “Show” on page 429 for more information.

Database Flush

Use this command to flush all cache entries for a Broadcast Manager Protocol.

Syntax:

database flush *protocol*

Where *protocol* is one of:

- IP
- IPX
- NetBIOS
- Source Route Management

Database List

Use this command to list general information about all entries in a given database, or to list detailed information about a user-specified entry in a database.

Syntax:

database list all . . .

specific . . .

all *database*

Lists general information about all entries in the specified database. Valid databases are:

- Bus-Filter filter items
- Bus-Police list
- BCM-Learned-MAC
- IP
- IPX
- IPX-server-farms
- LEC
- NetBIOS
- Registered-MAC
- Route-Descriptors
- Source Route Management

Note: The result of the **database list all** command is the same as the result of the **show** command. For example, **database list all ip** produces the same information as **show ip**.

Example:

```
database list all ip
Number of IP Addresses to display: 2

IP Address        MAC Address         TTL   Usage Count
---------------   -----------------   ---   -----------
9.67.195.1        10.00.5A.11.98.76     3            10
9.67.195.151      10.00.5A.49.13.4B     1             1
```

Where:

IP address
Is the IP address

MAC address
Is the MAC address associated with the IP address

TTL (Time to Live)
Is the amount of time (in minutes) remaining before this entry is removed from the cache.

Usage count
Is the number of times the entry was refreshed.

Example:

```
database list all lec
Number of LEC's to display: 2

    LEC-LES and LEC-BUS State  (UP=Up,  ID=Idle,  --. --.
      **=Other; Show specific LEC to see actual)    v   v
                                                   LEC    State   #ATM  #Reg   #Lrnd
LEC Primary ATM Address               Proxy  ID    LES BUS  Adrs  MACs    MACs
----------------------------------------  -  ----   --  --  ----  -----  -----
39999999999999000009999310110005AF972A000  Y  0001   UP  UP     1      5      0
39999999999999000009999310100041347323102  Y  0002   UP  UP     1      1      0
```

Where:

LEC primary ATM address
Is the primary ATM address of the LEC

Proxy Indicates whether or not this LE Client is a proxy LEC. A proxy LEC responds to LE ARP Requests for MAC addresses which it serves. These MAC addresses are not registered with the LES.

LEC ID
Is the LE Client Identifier

State LES
Is the operational state of the LEC at the LES. Possible states are:

- UP
- ID
- ** Other (to see this state use the **show specific LEC** command.)

State BUS
Is the operational state of the LEC at the BUS. Possible states are:

- UP = Up

- ID = Idle
- ** = Other (to see this state, use the **show specific LEC** command.)

Number of ATM addresses
Is the number of ATM addresses associated with the LEC.

Number of registered MACs
Is the number of registered MAC addresses associated with the LEC.

Number of learned MACs
Is the number of BCM–learned MAC addresses associated with the LEC.

specific *database*
Lists detailed information about a user specified entry. Valid databases are:

- IP
- IPX
- LEC
- MAC
- NetBIOS
- Route-Descriptor

Note: The result of the **database list specific** command is the same as the result of the **show specific** command. For example, **database list specific 1.2.3.4** produces the same information as **show specific ip 1.2.3.4**.

Example:

```
database list specific ip
   IP address [0.0.0.0]? 7.7.7.7
   IP Address:                    7.7.7.7
      MAC Address:                10.00.5A.BA.D0.88
      MAC Address Type:           Registered
      LEC ATM Address:            39999999999999000099990102100051591762 02
      LEC ID:                     0x0001
      LEC State at LES:           OPERATIONAL
      LEC State at BUS:           OPERATIONAL
      If dormant, proto ages in:  4 minute(s)
      Usage Count:                1
      SRM Ring Number:            unknown
```

Where:

IP address
Is a user entered IP address.

MAC address
Is the MAC address associated with the IP address.

MAC address type
Is the database entry type. Possible values are:

Registered
an entry registered by the LEC

Static Volatile
an entry created by the network manager

BCM Learned
an entry learned by the Broadcast Manager

Unknown
an entry of an unknown type

LE Services monitoring commands

LEC ATM address
Is the primary ATM address of the LEC that has the given MAC address.

LEC ID
Is the LE Client Identifier

LEC state at LES
Is the operational state of the LEC at the LES. Possible states are:

IDLE the LES-BUS is not active.

JOINING
A Control Direct VCC was accepted.

JOIN REJECTED
A Join request was rejected.

JOIN VERIFICATION
A request was sent to the LECS to validate the LEC's join request.

SIGNAL WAIT
The LES is waiting for completion of an in-progress call to establish a first leaf of Control Distribute VCC.

SIGNALLING
The LES is initiating signalling to establish a Control Distribute VCC to the LEC.

ADD PARTY RETRY
The LES is delaying the Add Party request for adding this LEC on the Control Distribute VCC. Congestion is suspected in the ATM switch network. The Add Party request will take place after a random delay.

OPERATIONAL
The Join was successful.

UNKNOWN
Indicates an unknown state.

LEC state at BUS
Is the operational state of the LEC at the BUS. Possible states are:

IDLE A control Direct VCC was accepted, or a Multicast VCC to LEC was released.

SIGNAL WAIT
The BUS is waiting for completion of an in-process call to establish the first leaf of Multicast Forward VCC.

SIGNALLING
The BUS initiated signalling to establish Multicast Forward VCC to LEC.

ADD PARTY RETRY
The BUS is delaying the Add Party request for adding this LEC on the Multicast Forward VCC. Congestion is suspected in the ATM switch network. The Add Party request will take place after a random delay.

OPERATIONAL
A Multicast Forward VCC to the LEC was successfully established.

UNKNOWN
Indicates an unknown state.

If dormant, proto ages in
Is the amount of time (in minutes) remaining before this entry is removed from the cache.

Usage count
Is the number of times entry was refreshed

SRM ring number
For SRM, 802.5 ring number where IP address is located

Example:

```
database list specific lec lecid
LECID [0001]?
LEC ID:                     0x0001
   LEC ATM Address:         39999999999999000099993101100005AF972A000
   Proxy:                   Yes
   LEC State at LES:        OPERATIONAL
   Entered LES State at:    00.00.03.46   (System Up Time)
   LEC State at BUS:        OPERATIONAL
   Entered BUS State at:    00.00.03.51   (System Up Time)
   Control Direct Vcc:      OPERATIONAL  0/193
   Control Distribute Vcc:  OPERATIONAL  0/194
   Multicast Send Vcc:      OPERATIONAL  0/195
   Multicast Forward Vcc:   OPERATIONAL  0/196
   MAC Address in Join Req: none
   Packet Tracing Eligible: No
   Add Party Being Delayed: No
   # ATM Address Mappings:  1
   # MAC Address Mappings:  5
   # RD Mappings:           1
   # BCM Learned MAC Addrs: 4
   # BCM Protocol Mappings: 4
   # BCM IPX Routers/Srvrs: 4
   IPX Server Farm Detected:No
   # SRM Ring Mappings:     2
   # TLVs registered:       0
```

Where:

LEC ID
Is the LE Client Identifier

LEC ATM address
Is the ATM address of the LEC

Proxy Indicates whether this LEC is a proxy LEC. Proxy LECs respond to LE ARP Requests for MAC addresses they serve. These MAC

LEC state at LES
Indicates the operational state of the LEC at the LES. Possible states are:

IDLE the LEC is not connected to either the LES or the BUS.

JOINING
A Control Direct VCC was accepted.

JOIN REJECTED
A Join request was rejected.

JOIN VERIFICATION
A request was sent to the LECS to validate the LEC's join request.

SIGNAL WAIT
The LES is waiting for completion of an in-progress call to establish a first leaf of Control Distribute VCC.

SIGNALLING
The LES is initiating signalling to establish a Control Distribute VCC to the LEC.

ADD PARTY RETRY
The LES is delaying the Add Party request for adding this LEC on the Control Distribute VCC. Congestion is suspected in the ATM switch network. The Add Party request will take place after a random delay.

OPERATIONAL
The Join was successful.

UNKNOWN
Indicates an unknown state.

Entered LES state at
Is the System Up Time at which LEC changed into its current state at the LES. Time is in *hours.minutes.seconds.hundredths* format.

LEC state at BUS
Is the operational state of the LEC at the BUS. Possible states are:

IDLE A Control Direct VCC was accepted, or a Multicast VCC to LEC was released.

SIGNAL WAIT
The BUS is waiting for completion of an in-progress call to establish the first leaf of Multicast Forward VCC.

SIGNALLING
The BUS initiated signalling to establish Multicast Forward VCC to LEC.

ADD PARTY RETRY
The BUS is delaying the Add Party request for adding this LEC on the Multicast Forward VCC. Congestion is suspected in the ATM switch network. The Add Party request will take place after a random delay.

OPERATIONAL
A Multicast Forward VCC to the LEC was successfully established.

UNKNOWN
Indicates an unknown state.

Entered BUS state at
Is the time that the LEC changed into its current state at the BUS. Time is in hours.minutes.seconds.hundredths format.

MAC address in Join Req
The MAC address in the Join Request, if present.

Packet tracing eligible
Indicates whether packets are eligible for tracing, provided ELS trace events are enabled.

Add Party Being Delayed
Indicates whether this LEC's request to join the ELAN is being delayed to help alleviate congestion which is suspected in the ATM switch network.

 # ATM address mappings
Is the number of ATM addresses associated with this LEC.

 # MAC address mappings
Is the number of MAC addresses associated with this LEC.

 # RD mappings
Is the number of route descriptors associated with this LEC.

 # BCM learned MAC addrs
Is the number of Broadcast Manager–learned MAC addresses associated with this LEC.

 # BCM protocol mappings
Is the number of protocols mapped to this LEC.

 # BCM IPX Routers/Srvrs
Is the number of IPX Routers and Servers associated with this LEC dynamically discovered by BCM IPX.

IPX Server Farm detected
Indicates whether the LEC is considered an IPX Server Farm from the perspective of BCM IPX. An IPX Server Farm can be detected behind a LEC either dynamically via the IPX Server Farm Detection function, or statically by configuring a BCM IPX Static Target for this LEC using a broadcast MAC address.

 # SRM ring mappings
Is the number of Source Route Management ring numbers associated with this LEC.

 # TLVs registered
Is the number of Type/Length/Value elements contained in this LEC's Join Request. If any TLVs are present, they are displayed as well.

Example:

```
database list specific mac
Registered or BCM Learned MAC Address: []? 10.00.5A.BA.D0.88
Registered MAC Address:     10.00.5A.BA.D0.88
   LEC ATM Address:         39999999999999000099990102100051591762 02
   Registering ATM Address: 39999999999999000099990102100051591762 02
   LEC ID:                  0x0001
   Entry Type:              Registered
   LEC State at LES:        OPERATIONAL
   LEC State at BUS:        OPERATIONAL
   SRM Ring Number:         unknown
   # BCM Protocol Mappings: 1
       IPX Network / Node Number:      00.00.77.77 / 10.00.5A.BA.D0.88
```

Where:

BCM learned MAC address
Is the Broadcast Manger–learned MAC address. This field is displayed for learned MAC addresses only.

Registered MAC address
Is the registered MAC Address. This field is displayed for registered MAC addresses only.

Registering ATM address
Is an ATM address of the LEC that registered the MAC address. This field is displayed for registered MAC addresses only.

Entry type
Is the Database entry type. Possible values are:

Registered
Registered entry (Entry was registered by a LEC)

Static Volatile
Static volatile entry (Entry was created by the network manager)

LEC ATM address
Is the ATM address of the LEC that has the given MAC address.

LEC ID
Is the LE Client Identifier.

LEC state at LES
Is the operational state of the LEC at the LES. Possible states are:

IDLE the LEC is not connected to either the LES or the BUS.

JOINING
A Control Direct VCC was accepted.

JOIN REJECTED
A Join request was rejected.

JOIN VERIFICATION
A request was sent to the LECS to validate the LEC's join request.

SIGNAL WAIT
The LES is waiting for completion of an in-progress call to establish a first leaf of Control Distribute VCC.

SIGNALLING
The LES is initiating signalling to establish a Control Distribute VCC to the LEC.

ADD PARTY RETRY
The LES is delaying the Add Party request for adding this LEC on the Control Distribute VCC. Congestion is suspected in the ATM switch network. The Add Party request will take place after a random delay.

OPERATIONAL
The Join was successful.

UNKNOWN
Indicates an unknown state.

LEC state at BUS
Is the operational state of the LEC at the BUS.

Possible states are:

IDLE A Control Direct VCC was accepted, or a Multicast VCC to LEC was released.

SIGNAL WAIT
The BUS is waiting for completion of an in-progress call to establish the first leaf of Multicast Forward VCC.

SIGNALLING
The BUS initiated signalling to establish Multicast Forward VCC to LEC.

ADD PARTY RETRY
The BUS is delaying the Add Party request for adding this LEC on the Multicast Forward VCC. Congestion is suspected in the ATM switch network. The Add Party request will take place after a random delay.

OPERATIONAL
A Multicast Forward VCC to the LEC was successfully established.

UNKNOWN
Indicates an unknown state.

SRM ring number
For SRM, the 802.5 ring where the registered or BCM-Learned MAC address is located.

 # BCM protocol mappings
Is the number of protocols mapped to this MAC address. A list of the protocol mappings will be displayed. The possible mappings are:

- IPX Network / Node Number
- IP address
- NetBIOS name string
- NetBIOS name in hex (shown only if NetBIOS name string has unprintable characters)

Delete

Use the **delete** command to stop the LES-BUS and remove it from the active configuration. (The LES-BUS definition remains in static RAM). If the **delete** command is issued and you then want to start the LES-BUS, without restarting the MSS Server, you must issue the **create** command.

Syntax:

delete

Example:

```
EXISTING LES-BUS 'losangeles'+ delete
Are you sure you want to delete this LES/BUS? [No]:
LES/BUS:'losangeles':not deleted
```

Disable

Use the **disable** command to disable various LES-BUS functions.

You can dynamically disable Broadcast Manager (IP, IPX, IPX Server Farm Detection, or NetBIOS), BUS Monitor, BUS Police, individual filter items for BUS filter, Redundancy, Security, or Source Route Manager. Disabling of the chosen

option occurs immediately, but the LES-BUS's configured state in Static RAM does not change. If you wish to change permanently the configured state in Static RAM, use the `config>` interface.

Syntax:

disable **bcm**
bus-filter
bus-monitor
bus-police
redundancy
security
source

bcm Disables broadcast management for:

- all
- ip
- ipx
- ipx-server-farm
- netbios

bus-filter
Disables Bus filtering.

bus-monitor
Disables the BUS Monitor.

bus-police
Disables BUS Police.

redundancy
Disables LES-BUS redundancy

security
Disables LES-BUS security

source route management
Disables source route management

Example:

```
EXISTING LES-BUS 'losangeles'+ disable ?
BCM
BUS-FILTER
BUS-MONITOR
BUS-POLICE
FILTER-ITEM in bus filter
REDUNDANCY
SECURITY (LECS validation of Joins)
SOURCE route management
EXISTING LES-BUS 'losangeles'+ disable bcm ?
ALL
IP
IPX
IPX-Server-Farm detection
NETBIOS
EXISTING LES-BUS 'losangeles'+disable bcm all
LES/BUS: 'losangeles' : Disable BCM for IP successful
LES/BUS: 'losangeles' : Disable BCM for IPX successful
LES/BUS: 'losangeles' : Disable BCM for NetBIOS successful
EXISTING LES-BUS 'losangeles'+ disable bcm ip
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+ disable bcm ipx
```

```
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+ disable bcm ipx-server-farm
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+ disable bcm netbios
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+ disable bus-monitor
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+ disable bus-police
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+ disable bus-filter
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+ disable redundancy
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+ disable security
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+ disable source
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+
```

Enable

Use the **enable** command to enable various LES-BUS functions. You may dynamically enable Broadcast Manager (IP, IPX, IPX Server Farm Detection, or NetBIOS), BUS Monitor, Redundancy, Security (LECS validation of Joins), or Source Route Manager. The chosen option is enabled immediately, but the LES-BUS's configured state in Static RAM does not change. If you wish to change permanently the configured state in Static RAM, you should use the `config>` interface.

Notes:

1. You cannot enable the Broadcast Manager while the BUS is in *Adapter* or *VCC-Splice* mode.
2. You cannot enable the BUS-Monitor while the BUS is in *VCC-Splice* mode.
3. You cannot enable BUS-Police while the BUS-Monitor is not enabled.

Syntax:

enable **bcm**
bus-filter
bus-monitor
bus-police
redundancy
security
source

bcm Enables broadcast management for:

- all
- ip
- ipx
- ipx-server-farm
- netbios

bus-filter *item*
Enables the bus-filter.

bus-monitor
Enables the BUS Monitor.

LE Services monitoring commands

bus-police
Enables BUS Police.

redundancy
Enables LES-BUS redundancy

security
Enables LES-BUS security

source route management
Enables source route management

Example:

```
EXISTING LES-BUS 'losangeles'+ enable ?
BCM
BUS-MONITOR
REDUNDANCY
SECURITY (LECS validation of Joins)
SOURCE route management
EXISTING LES-BUS 'losangeles'+enable bcm ?
ALL
IP
IPX
IPX-SERVER-FARM detection
NETBIOS
EXISTING LES-BUS 'losangeles'+enable bcm all
LES/BUS: 'losangeles' : Enable BCM for IP successful
LES/BUS: 'losangeles' : Enable BCM for IPX successful
LES/BUS: 'losangeles' : Enable BCM for NetBIOS successful
EXISTING LES-BUS 'losangeles'+enable bcm ip
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+enable bcm ipx
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+enable bcm ipx-server-farm
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'enable bcm netbios
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+enable bus-filter
EXISTING LES-BUS 'losangeles'+enable bus-monitor
EXISTING LES-BUS 'losangeles'+enable bus-police
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+enable redundancy
  (  1) Primary LES-BUS
  (  2) Backup LES-BUS
Redundancy Role [1]?
Enable Peer Redundancy Option? [No]: yes
ATM address of backup LES-BUS [39.84.0F.00.00.00.00.00.00.00.00.00.02.22.33.44.55.66.77.02]?
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+
EXISTING LES-BUS 'losangeles'+ enable redundancy
  (  1) Primary LES-BUS
  (  2) Backup LES-BUS
Redundancy Role [1]? 2
Backup LES/BUS is now capable of Peer Redundancy.
Enable Peer Redundancy at Primary LES/BUS, if desired.
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+
EXISTING LES-BUS 'losangeles'+enable security
LES/BUS: 'losangeles' : parameter successfully set
EXISTING LES-BUS 'losangeles'+enable source
LES/BUS: 'losangeles' : parameter successfully set
```

List

Use the **list** command to list the LES-BUS's status and currently running configuration parameters.

Syntax:

list

Example:

```
LES-BUS config for ELAN 'elan01'> list
ELAN Name:                elan01
   ELAN Type:             Ethernet
   ATM Device number:     0
   # of Proxy LEC's:      0
   # of Non-Proxy LEC's:  0
   LES ATM Address:       39999999999999000099990200000 4AC47391803

-Status-
   LES-BUS State:                      OPERATIONAL
   Able to accept new LEC's:           NO (Redundant)
   # of LEC's last reported by Partner: 2
   Enhanced Redundancy VCC State:      OPERATIONAL
   Major Reason LES-BUS was last Down:  none
   Minor Reason LES-BUS was last Down:  none
   LES-BUS State last changed at:      00.08.53.30   (System Up Time)
   LES-LEC Status Table changed at:    00.09.17.43   (System Up Time)
   BUS-LEC Status Table changed at:    00.09.17.43   (System Up Time)
   UNI Version:                        3.0
   IP BCM:                             INACTIVE
   IPX BCM:                            INACTIVE
   NetBIOS BCM:                        INACTIVE

-Current Configuration-
   LES-BUS Enabled/Disabled:                  Enabled
   ATM Device number:                         0
   End System Identifier (ESI):               00.04.AC.47.39.18
   Selector Byte:                             0x03
   ELAN Type:       (S2)                      Ethernet
   Max Frame Size:  (S3)                      1516
   Control Timeout: (S4)                      120
   Max Frame Age:   (S5)                      1
   ELAN Identifier: (S7)                      2
   Mcast Send Disconnect Timeout: (S9)        60
   LECID Range Minimum:                       0x0001
   LECID Range Maximum:                       0xFEFF
   Validate Best Effort Peak Cell Rate (PCR): No
   Control Distribute VCC Traffic Type:       Best Effort VCC
   Control Distribute VCC PCR in Kbps:        155000
   Control Direct VCC Max Reserved Bandwidth: 0
   Multicast Forward VCC Traffic Type:        Best Effort VCC
   Multicast Forward VCC PCR in Kbps:         155000
   Multicast Send VCC MAX Reserved Bandwidth: 0

    -LES-BUS Options-
   BUS Mode:                                  Adapter
   Security (LECS Validation of Joins):       Disabled
   Partition LE_ARP_REQUEST Forwarding Domain: Yes
   LE_ARP RESPONSE Destination:               One client
   Partition Unicast Frame Domain:            Yes
   Redundancy:                                Enabled
   Peer Redundancy:                           (Backup always Peer Enabled)
   Redundancy Role:                           Backup LES-BUS
   ATM address trace filter value: 00000000000000000000000000000000000000000000
   ATM address trace filter mask:  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

    -BUS Monitor Configuration-
   Monitor Host Usage of BUS:                 Disabled
   # Top Hosts to Record:                     10
   # Seconds in each sample interval:         10
   # Seconds between sample intervals:        1800
   Frame sampling rate:                       1 out of 10

    -Broadcast Manager Configuration-
   IP BCM:                                    Disabled
   IPX BCM:                                   Disabled
   NetBIOS BCM:                               Disabled
   BCM IP Cache Aging Time:                   5
   BCM IPX Cache Aging Time:                  3
   BCM NetBIOS Cache Aging Time:              15
   BCM IPX Maximum Forwarding List:           50
   BCM IPX Server Farm Detection:             Disabled
   BCM IPX Server Farm Threshold:             20
   No BCM IPX Static Entries defined

    -Bus Filter Configuration-
   Bus Filter Enabled:                        Disabled
   Bus Filter's Preferred List                EXCLUDE LIST
   Bus Filter's Default Action                EXCLUDE

    -Bus Police Configuration-
   Bus Police Enabled:                        Disabled
   Bus Police Filter Duration                 TEMPORARY
   Bus Police Threshold (packets/sec)         0
 LES-BUS config for ELAN 'elan01'>
```

Where:

LES-BUS State
is the operational state of the LES-BUS. Possible states are:

IDLE LES-BUS not active.

INITIALIZATION
LES-BUS control block is being initialized.

ATM ADDR ACTIVATION
LES-BUS ATM addresses are being activated.

GET UNI VERSION
Getting UNI version that is being run.

GOT UNI VERSION
UNI version has been determined.

OPERATIONAL
LES-BUS state is up or operational.

ATM ADDR DEACTIVATED
ATM address deactivated by switch.

NET DOWN
ATM interface not operational.

ERROR /DOWN
The operation of LES-BUS instance terminated due to fatal error.

UNKNOWN
Unknown state.

Able to accept new LEC's
Identifies the ability for the LES-BUS to accept new LE Clients. Possible values are:

- YES
- NO (Redundant)
- NO (not Operational)

# of LEC's last reported by Partner
Specifies the number of LE Clients joined to the Partner LES-BUS if this LES-BUS is currently Redundant.

Redundancy VCC State
Identifies the state of the LES-BUS Redundancy VCC. Possible values are:

- IDLE
- SIGNALLING
- RELEASED
- ESTABLISHED

If both the Primary and backup LES-BUSs are capable of the Enhanced Redundancy function, and are in communication via the Enhanced Redundancy VCC, this line in the list will be shown as *Enhanced Redundancy VCC State: OPERATIONAL*.

Major Reason LES-BUS was last Down
is the reason why the LES-BUS was last down, if ever.

Minor Reason LES-BUS was last Down
contains additional information about why the LES-BUS was last down, if ever.

LES-BUS State last changed at
is the system up time at which the LES-BUS entered its current state. The format is *hours.minutes.seconds.hundredths*

LES-LEC Status Table changed at
is the most recent system up time at which a LEC's state changed at the LES.

BUS-LEC Status Table changed at
is the most recent system up time that a LEC entered or exited operational state at the BUS.

IP BCM
The current status of IP BCM.

IPX BCM
The current status of IPX BCM. IPX BCM can only be *ACTIVE* if IPX BCM is configured to Enabled, the LES-BUS State is Operational, and if the **IPX BCM Active Forwarding List Size** has not exceeded its configured threshold, **BCM IPX Maximum Forwarding List**. See on page 371 for additional information.

NetBIOS BCM
The current status of NetBIOS BCM.

IPX BCM Active Forwarding List Size
The number of entries currently in IPX BCM's Forwarding List. If this number exceeds the configured threshold for **BCM IPX Maximum Forwarding List**, IPX BCM will become *INACTIVE*, and the BUS will forward all IPX broadcast frames. Note that this information is only displayed if IPX BCM is currently *ACTIVE*.

See "Configuration Commands for a LES-BUS" on page 354 for more information about the configuration parameters.

Restart

Use the **restart** command to restart a running or stopped LES-BUS. A LES-BUS can be restarted using the parameters configured under the `Talk 5` or `Talk 6` interface.

Syntax:

restart	*t5*
	t6

Example:

```
EXISTING LES-BUS 'elan01'+restart ?
T5 (Using config parms in Talk 5)
T6 (Using config parms written in Talk 6)
EXISTING LES-BUS 'elan01'+restart t5
Are you sure you want to restart this LES/BUS? [No] : yes
LES/BUS: 'elan01': RESTARTING


EXISTING LES-BUS 'elan01'+restart t6
Are you sure you want to restart this LES/BUS? [No] : yes
LES/BUS: 'elan01': RESTARTING
```

Set

Use the **set** command to dynamically set the values of various LES-BUS configuration parameters.

Syntax:

set	bus-monitor *settings*
	control *timeout*
	frame-age
	ip *broadcast cache age*
	ipx-broadcast *cache age*
	ipx-maximum *size of forwarding list*

ipx-server-farm *threshold*

le-arp *response destination*

multicast-send-disconnect-timeout

netbios *broadcast cache age*

trace

traffic *type*

You can dynamically set the following LES-BUS configuration parameters. The parameter that you set is immediately used by the LES-BUS, however the LES-BUS's configured parameter values in Static RAM do not change. To permanently change the configured state in Static RAM, use the `config>` interface.

See 367 for detailed information about the **set** parameters.

```
 EXISTING LES-BUS+ set ?
  BUS-MONITOR settings
  CONTROL timeout
  FRAME-AGE
  IP broadcast cache age
  IPX broadcast cache age
  IPX-SERVER-FARM threshold
  LE ARP response destination
  MULTICAST send disconnect time
  NETBIOS broadcast cache age
  TRACE
  TRAFFIC type

EXISTING LES-BUS+ set bus-monitor ?
DURATION-OF-SAMPLE    (# Seconds in each sample interval)
SAMPLE-RATE           (Frame sampling rate)
TIME-BETWEEN-SAMPLES  (# Minutes between sample intervals)
TOP-NUMBER-MACS       (# Top Hosts to Record)

EXISTING LES-BUS+ set bus-monitor duration
Duration of sample interval in seconds (1-600) [10]?
LES-BUS: 'test' : parameter successfully set

EXISTING LES-BUS+ set bus-monitor sample
Frame sampling rate (1-1000) [10]?
LES-BUS: 'test' : parameter successfully set

EXISTING LES-BUS+ set bus-monitor time
Number of seconds between sample intervals (2-7200) [1800]?
LES-BUS: 'test' : parameter successfully set

EXISTING LES-BUS+ set bus-monitor top
Number of top MAC addresses to record (1-100) [10]?
LES-BUS: 'test' : parameter successfully set

EXISTING LES-BUS+ set control
Control timeout (10-300) [110]? 120
LES-BUS: 'test' : parameter successfully set

EXISTING LES-BUS+ set frame-age
Maximum frame age (1-4) [1]?
LES-BUS: 'test' : parameter successfully set

EXISTING LES-BUS+ set ip
IP cache age, in minutes (2-20) [5]?
LES-BUS: 'test' : parameter successfully set

EXISTING LES-BUS+ set ipx
IPX cache age, in minutes (1-10) [3]?
LES-BUS: 'test' : parameter successfully set

EXISTING LES-BUS+ set ipx-server-farm
IPX Server Farm Threshold (2 -50) [20]?10
LES-BUS: 'test' : parameter successfully set

EXISTING LES-BUS+ set le
  (  1) One client
  (  2) All clients
LE ARP response destination [1]?
LES-BUS: 'test' : parameter successfully set

EXISTING LES-BUS+ set multicast
Multicast Send disconnect time [60]?
LES-BUS: 'test' : parameter successfully set

EXISTING LES-BUS+ set netbios
NetBIOS cache age, in minutes (10-20) [15]?
LES-BUS: 'test' : parameter successfully set

EXISTING LES-BUS+ set trace ?
MASK
VALUE

EXISTING LES-BUS+ set trace mask
ATM address trace filter mask [FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF]?
LES-BUS: 'test' : parameter successfully set

EXISTING LES-BUS+ set trace value
ATM address trace filter value [00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00]?
LES-BUS: 'test' : parameter successfully set

EXISTING LES-BUS+ set traffic ?
```

```
MAXIMUM reserved bandwidth
VALIDATE peak cell rate


EXISTING LES-BUS+ set traffic maximum ?
CONTROL Direct VCC maximum
MULTICAST Send VCC maximum

EXISTING LES-BUS+ set traffic maximum control
Maximum reserved bandwidth in Kbps (0 - 155000) [0]?
LES-BUS: 'test' : parameter successfully set

EXISTING LES-BUS+ set traffic maximum multicast
Maximum reserved bandwidth in Kbps (0 - 155000) [0]?
LES-BUS: 'test' : parameter successfully set

EXISTING LES-BUS+ set traffic validate
Validate peak cell rate of best effort VCCs? [No]:
LES-BUS: 'test' : parameter successfully set
```

Show

Use the **show** command to display various information related to this LES-BUS. The **show** command consolidates other LES-BUS Console display commands and uses a shorter command syntax.

The **show** commands are equivalent to other commands contained in this chapter. For example, **show lec** is equivalent to **database list all lec**. See “Database List” on page 413 for additional information.

Syntax:

show

- bcm-learned-mac *entries*
- bus-filter *filteritems*
- bus-police *lists*
- current
- ip *entries*
- ipx-server-farms
- lec *entries*
- netbios *entries*
- registered-mac *entries*
- route-descriptor *entries*
- source route management
- specific *entry*
- statistics
- vccs *opened*

Example:

```
EXISTING LES-BUS 'losangeles'+show ?
BCM-LEARNED-MAC entries
BUS-FILTER filter items
BUS-POLICE lists
CURRENT configuration of LES-BUS
IP entries
IPX entries
IPX-server-farms
```

```
LEC entries
NETBIOS entries
REGISTERED-MAC entries
ROUTE-DESCRIPTOR entries
SOURCE route management
SPECIFIC entry
STATISTICS
VCCs opened
```

bcm-learned-mac

bus-filter
Displays information about configured bus filters.

bus-police
Displays information about the configuration of BUS Police.

current
This command is equivalent to **list**. See “List” on page 424 for additional information.

Example:

```
EXISTING LES-BUS 'losangeles'+show current
```

ip

ipx

ipx-server-farms

lec

netbios

registered-mac

route-descriptor

source route management

statistics *type*
This command is equivalent to **statistics display** *type*, where *type* can be one of the following:

- BCM
- BUS monitor: Top N users
- LES-BUS
- Source route management

See 432 for additional information.

Example:

```
EXISTING LES-BUS 'losangeles'+show statistics bcm all
```

vccs opened
Displays the VCCs that have been opened.

Example:

```
EXISTING LES-BUS 'losangeles'+show vccs
ELAN Name:                losangeles

                                      VCC State  VPI/VCI
  Point-to-multipoint VCCs           -----------  -------
    LES Control Distribute VCCs
      LUNI Version 1
        All Clients:                       IDLE    0/0
        Non-proxy Clients:                 IDLE    0/0
        Proxy Clients                      IDLE    0/0
      LUNI Version 2
        All Clients                        IDLE    0/0
```

```
        Non-proxy Clients:              IDLE    0/0
        Proxy Clients:                  IDLE    0/0
    BUS Multicast Forward VCCs
        All Clients:                    IDLE    0/0
        Non-proxy Clients:              IDLE    0/0
        Proxy Clients:                  IDLE    0/0

  Point-to-Point VCCs
    LES Enhanced Redundancy:      OPERATIONAL    0/194

                                    Valid  No. of VCCs
  Group VCCs                        -----  -----------
    LES Control Distribute VCCs
        All Clients:                  Yes            1
        Proxy Clients:                Yes            0
        Version 1 Clients:            Yes            0
        Version 2 Clients:            Yes            1
    BUS Multicast Forward VCCs
        All Clients:                  Yes            1
 EXISTING LES-BUS 'losangeles'+
```

Statistics

Use the **statistics** command to either clear or display statistics associated with LAN Emulation MIBs. Some of the fields displayed by the **statistics** command correspond to specific MIB entries that are in **ibmlesrv.mib** located at **ftp://ftp.nways.raleigh.ibm.com/pub/netmgmt/mss/**.

Syntax:

statistics	clear ...
	display ...

The **statistics clear** command zeroes statistical data that previously was gathered for BCM, LES-BUS, or Source Route Management.

Note: Some LES-BUS counters, such as the number of proxy LECs, are not cleared, since they have other function in addition to maintaining statistical data.

Syntax:

clear	bcm *protocol*
	les-bus *type*
	source *protocol*

Where *protocol* or *type* can be:

	protocol or type
clear bcm	all
	ip
	ipx
	netbios
clear les	bus
	lec-bus *atm-address*
	lec-bus *lecid*
	lec-les *atm-address*
	lec-les *lecid*

	les
clear source	all
	ip
	ipx
	netbios

Example:

```
Existing LES-BUS+ statistics clear bcm all
Existing LES-BUS+
```

The **statistics display** command provides statistical data for BCM, LES-BUS, and Source Route Management.

Syntax:

statistics display	bcm *protocol-stats*
	bus monitor
	les-bus *type*
	source *protocol-stats*

Where *protocol-stats* can be:

protocol-stats

statistics display bcm
- all
- ip
- ipx
- netbios

statistics display source
- all
- ip
- ipx
- netbios

or where *type* can be:

	type
statistics display les-bus	bus
	lec-bus *atm-address*
	lec-bus *lecid*
	lec-les *atm-address*
	lec-les *lecid*
	les

Example:

```
EXISTING LES-BUS+ statistics display bcm all

                                                                Total BCM
                                IP         IPX     NetBIOS   Processed
                        ----------  ----------  ----------  ----------
 inFrms:                  182972         324         374      299518
 inOctets:              11410392       36798       32840    22342391
 inReturns:               129888           6         334      246076
 inReturnOctets:         8113160         564       30254    19006339
 inFiltered:                   0           0          40          40
 inFilteredOctets:             0           0        2586        2586
 outFrms:                  53084         318           0       53402
 outFrmsOctets:          3297232       36234           0     3333466
 outError:                     0           0           0           0
 outErrorOctets:               0           0           0           0
```

The statistical counters for the **statistics display bcm all** command map to MIB variables as follows:

```
Total BCM Processed
Displayed Name                        MIB ENTRY
---------------------                 ---------
inFrms                               bcmFramesReceived
inOctets                             bcmOctetsReceived
inReturns                            bcmFramesReturned
inReturnOctets                       bcmOctetsReturned
inFiltered                           bcmFramesDiscarded
inFilteredOctets                     bcmOctetsDiscarded
outFrms                              bcmFramesTransmitted
outFrmsOctets                        bcmOctetsTransmitted
outError                             bcmTransmitErrorFrames
outErrorOctets                       bcmTransmitErrorOctets

IP DISPLAYED NAME                      MIB ENTRY
-----------------                      ---------
inFrms                               bcmIpFramesReceived
inOctets                             bcmIpOctetsReceived
inReturns                            bcmIpFramesReturned
inReturnOctets                       bcmIpOctetsReturned
inFiltered                           bcmIpFramesDiscarded
inFilteredOctets                     bcmIpOctetsDiscarded
outFrms                              bcmIpFramesTransmitted
outFrmsOctets                        bcmIpOctetsTransmitted
outError                             bcmIpTransmitErrorFrames
outErrorOctets                       bcmIpTransmitErrorOctets

IPX DISPLAYED NAME                     MIB ENTRY
-----------------                      ---------
inFrms                               bcmIpxFramesReceived
inOctets                             bcmIpxOctetsReceived
inReturns                            bcmIpxFramesReturned
inReturnOctets                       bcmIpxOctetsReturned
inFiltered                           bcmIpxFramesDiscarded
inFilteredOctets                     bcmIpxOctetsDiscarded
outFrms                              bcmIpxFramesTransmitted
outFrmsOctets                        bcmIpxOctetsTransmitted
outError                             bcmIpxTransmitErrorFrames
outErrorOctets                       bcmIpxTransmitErrorOctets


NetBIOS DISPLAYED NAME                   MIB ENTRY
----------------------                   ---------
inFrms                               bcmNbFramesReceived
inOctets                             bcmNbOctetsReceived
inReturns                            bcmNbFramesReturned
inReturnOctets                       bcmNbOctetsReturned
inFiltered                           bcmNbFramesDiscarded
inFilteredOctets                     bcmNbOctetsDiscarded
outFrms                              bcmNbFramesTransmitted
outFrmsOctets                        bcmNbOctetsTransmitted
outError                             bcmNbTransmitErrorFrames
outErrorOctets                       bcmNbTransmitErrorOctets
```

display bus

Displays statistical data associated with BUS Monitoring.

Example:

```
EXISTING LES-BUS+ statistics display bus
   -BUS Monitor Status-
   Currently in a sample interval ?            no
   Next sample interval scheduled in:          0 minute(s), 18 second(s)

   -Results of Last Complete Sample-
   BUS Monitor sample interval started at:     13.27.03.98   (System Up Time)
   Duration of sample interval:                59 second(s)
   # Top Hosts Actually Recorded:              5
   # Frames Received in sample interval:       301
   # Frames Sampled in sample interval:        301
   Frame sampling rate:                        1 out of 1
                                                                      # frames
Rank  Source MAC Addr.    Associated LEC ATM Address                   sampled
----  -----------------   ----------------------------------------   ----------
   1  10.00.5A.AA.AA.AA   39999999999999000099990101100 05A12340002          100
   2  10.00.5A.66.66.66   39999999999999000099990101100 05A12340002           60
   3  10.00.5A.EE.EE.EE   39999999999999000099990101100 05A12340002           52
   4  10.00.5A.55.55.55   39999999999999000099990101100 05A12340001           50
   5  10.00.5A.99.99.99   39999999999999000099990101100 05A12340001           39
EXISTING LES-BUS+
```

statistics display les lec-bus lecid

Lists the number of multicast, broadcast, and unknown forward requests received or discarded by the BUS from this LEC.

```
EXISTING LES-BUS+ statistics display les lec-bus lecid
LECID [0]? 1
ATM Forum LEC-BUS MIB Statistics:
   recvs:                              1
   discards:                           0
```

The statistical counters for some fields generated by the **statistics display les lec-bus** command map to MIB variables as follows:

```
LEC-BUS Displayed Name              MIB ENTRY
----------------------              ---------
recvs                               busLecRecv
discards                            busLecDiscards
```

statistics display [les bus or lec-bus or lec-les or les]

Displays statistical data for a given LEC or ELAN.

Example:

```
ATM Forum BUS MIB Statistics:
   inDiscards:                            0
   inOctets:                              0
   inUcastFrms:                           0
   inMcastFrms:                           0
   frmTimeouts:                           0
   mcastSendRefused:                      0
   mcastFwdFailure:                       0
Other Statistics:
   inExplorer:                            0
   inFlushReq:                            0
   outFlushReq_mcastFwd:                  0
   outFlushReq_mcastSend:                 0
   outUcastFrms_mcastFwd:                 0
   outUcastFrms_mcastSend:                0
   outMcastFrms:                          0
   outOctets:                             0
   mcastSendReleased:                     0
   mcastFwdReleased:                      0
   mcastFwdPartyReleased:                 0
   invalidProtocol_droppedFrames:         0
   verNotSup_droppedFrames:               0
   invalidOpcode_droppedFrames:           0
   invalidLecid_droppedFrames:            0
   invalidSize_droppedFrames:             0
   flushToBus_droppedFrames:              0
   incompleteSourceConnect_droppedFrames: 0
   incompleteTargetConnect_droppedFrames: 0
   noProxy_droppedFrames:                 0
   lecsWaitingForMcastFwd:                0
   mcastSendDisconnectTimeouts:           0
   badRifFrames:                          0
   flushTargetMismatch_droppedFrames:     0
   flushInvalidTag_droppedFrames:         0
   BusFilter_MatchOnExcludeList:          0
   BusFilter_MatchOnIncludeList:          0
   BusFilter_NoMatchSoExcludeFrame:       0
   BusFilter_NoMatchSoIncludeFrame:       0
   BusPolice_FramesDiscarded:             0
```

ATM Forum BUS MIB Statistics:

The statistical counters for some fields generated by the **statistics display les-bus bus** command map to MIB variables as follows:

BUS DISPLAYED NAME	MIB ENTRY
inDiscards	busStatInDiscards
inOctets	busStatInOctets
inUcastFrms	busStatInUcastFrms
inMcastFrms	busStatInMcastFrm
frmTimeouts	busStatFrmTimeOuts
mcastSendRefused	busStatMcastSendRefused
mcastFwdFailure	busStatMcastFwdFailure

Other Statistics:

The following definitions are not MIB-related:

inExplorer
Number of Token-Ring explorer frames received by BUS

inFlushReq
Number of Flush request control frames received by BUS

outFlushReq_mcastFwd
Number of Flush request control frames forwarded by BUS on Multicast Forward VCC(s)

outFlushReq_mcastSend
Number of Flush request control frames forwarded by BUS on Multicast Send VCC

outUcastFrms_mcastFwd
Number of unicast frames forwarded by BUS on Multicast Forward VCC(s)

outUcastFrms_mcastSend
Number of unicast frames forwarded by BUS on Multicast Send VCC

outMcastFrms
Number of multicast frames forwarded by BUS

outOctets
Number of octets forwarded by BUS (includes both control and data)

mcastSendReleased
Number of Multicast Send VCCs released by LEC/network for any reason

mcastFwdReleased
Number of Multicast Forward VCCs released by LEC/network for any reason (this is release of entire point-to-multipoint VCC, not just one party)

mcastFwdPartyReleased
Number of times call to party on Multicast Forward VCC was released by LEC/network for any reason

invalidProtocol_droppedFrames
Number of control frames dropped by BUS due to invalid protocol

verNotSup_droppedFrames
Number of control frames dropped by BUS due to incorrect version #

invalidOpcode_droppedFrames
Number of control frames dropped by BUS due to invalid opcode

invalidLecid_droppedFrames
number of frames (control or data) dropped by BUS due to invalid LECID

invalidSize_droppedFrames
Number of frames (control or data) dropped by BUS due to frame size being invalid

flushToBus_droppedFrames
Number of FLUSH request frames dropped by BUS because target ATM address was ATM address of BUS

incompleteSourceConnect_droppedFrames
Number of frames (control or data) dropped by BUS because source LEC had not completed the BUS connect phase

incompleteTargetConnect_droppedFrames
Number of frames (control or data) dropped by BUS because target LEC had not completed the BUS connect phase

noProxy_droppedFrames
Number of ″unknown″ FLUSH request or non-multicast data frames dropped by BUS because the ELAN had no proxy LEC members

lecsWaitingForMcastFwd
Number of LECs on this ELAN waiting to be added to the BUS Multicast Forward VCC due to the Add Party message being delayed due to suspected ATM switch congestion.

mcastSendDisconnectTimeouts
Number of times a LEC Multicast Send Disconnect Timer has expired. If the associated LEC had not reached full operational status with the BUS, the LEC was terminated from the ELAN.

badRifFrames
Number of frames received with bad RIFs.

Note: This only applies when BUS is configured to use a Partitioned Unicast Frame Domain and when the Local Segment Number is configured.

flushTargetMismatch_droppedFrames
Number of Flush frames with target LAN destination not registered by target ATM address.

flushInvalidTag_droppedFrames
Number of Flush frames with invalid tag in target LAN destination.

Example:

```
EXISTING LES-BUS+ statistics display les les
ATM Forum LES MIB Statistics:
   joinOK:                                 2
   verNotSup:                              0
   invalidReqParam:                        0
   dupLanDest:                             0
```

```
   dupAtmAddr:                          0
   insRes:                              0
   accDenied:                           0
   invalidReqId:                        0
   invalidLanDest:                      0
   invalidAtmAddr:                      0
   badPkts:                             0
   outRegFails:                         0
   leArpIn:                             2
   leArpFwd:                            0
Other Statistics:
   leArpAnswers:                        2
   leArpRspFwd:                         0
   topologyFwd:                         0
   narpFwd:                             0
   flushRspFwd:                         0
   outJoinFails:                        0
   regOK:                               2
   unRegOK:                             0
   outUnRegFails:                       0
   proxyLecs:                           1
   nonProxyLecs:                        0
   macAddrMappings:                     1
   rdMappings:                          0
   atmAddrMappings:                     1
   joinRetransmits:                     0
   joinParmChanges:                     0
   joinTimeouts:                        0
   reRegs:                              0
   ctlDirRefused:                       0
   ctlDirReleased_err:                  0
   ctlDistFailure:                      0
   ctlDistReleased_err:                 0
   ctlDistPartyReleased_err:            0
   redundancyVccRefused:                0
   redundancyVccReleased:               0
   redundancyVccFailure:                0
   oam_droppedFrames:                   0
   invalidSize_droppedFrames:           0
   invalidMarker_droppedFrames:         0
   invalidProtocol_droppedFrames:       0
   verNotSup_droppedFrames:             0
   invalidLecid_droppedFrames:          0
   unknownLecid_droppedFrames:          0
   invalidOpcode_droppedFrames:         0
   dupJoin_droppedFrames:               0
   incompleteSourceJoin_droppedFrames:  0
   incompleteTargetJoin_droppedFrames:  0
   noProxy_droppedFrames:               0
   lecsWaitingForCtrlDist:              0
   verifyOk:                            0
   outVerifyFails:                      0
   inRedundancyStatus:                  2088
   outRedundancyStatus:                 2087
```

ATM Forum LES MIB Statistics:

The statistical counters for some fields generated by the **statistics display les les** command map to MIB variables as follows:

LES DISPLAYED NAME	MIB ENTRY
joinOK	lesStatJoinOk
verNotSup	lesStatVerNotSup
invalidReqParam	lesStatInvalidReqParam
dupLanDest	lesStatDupLanDest
dupAtmAddr	lesStatDupAtmAddr
insRes	lesStatInsRes
accDenied	lesStatAccDenied
invalidReqId	lesStatInvalidReqId
invalidLanDest	lesStatInvalidLanDest
invalidAtmAddr	lesStatInvalidAtmAddr
badPkts	lesStatInBadPkts
outRegFails	lesStatOutRegFails
leArpIn	lesStatLeArpIn
leArpFwd	lesStatLeArpFwd

Other Statistics:

The following definitions are not MIB-related:

leArpAnswers
Number of ARP requests answered by LES

leArpRspFwd
Number of ARP responses forwarded by LES

topologyFwd
Number of topology frames forwarded by LES

narpFwd
Number of NARP frames forwarded by LES

flushRspFwd
Number of flush response frames forwarded by LES

outJoinFails
Number of join responses transmitted with unsuccessful status values, includes retransmissions

regOK
Number of successful registration responses sent by LES, includes re-registrations

unRegOK
Number of successful unregistration responses sent by LES

outUnRegFails
Number of unregistration responses transmitted with unsuccessful status values

proxyLecs
Number of Proxy LECs currently joined to LES

nonProxyLecs
Number of Non-Proxy LECs currently joined to LES

regMacAddr
Number of MAC address mappings currently in database

regRd Number of route descriptor mappings currently in database

regAtmAddr
Number of unique ATM addresses currently in mapping database

joinRetransmits
Number of join response retransmissions

joinParmChanges
Number of LEC ELAN memberships terminated because parameters changed on subsequent JOIN request

joinTimeouts
Number of join timeouts

reRegs
Number of re-registrations

ctlDirRefused
Number of Control Direct VCC call setup requests rejected by the LES for any reason

ctlDirReleased_err
Number of Control Direct VCCs released by LEC/network with cause code indicating error

ctlDistFailure
Number of Control Distribute VCC requests made by LES that failed for any reason (includes calls to first and subsequent parties)

ctlDistReleased_err
Number of Control Distribute VCCs released by

LEC/network due to error (this is release of entire point-to-multipoint VCC, not just one party)

ctlDistPartyReleased_err
Number of times call to party on Control Distribute VCC was released by LEC network with cause code indicating error

oam_droppedFrames
Number of OAM frames dropped by LES

invalidSize_droppedFrames
Number of frames dropped by LES due to frame size being invalid for a control frame

invalidMarker_droppedFrames
Number of frames dropped by LES due to invalid marker

invalidProtocol_droppedFrames
Number of frames dropped by LES due to invalid protocol

verNotSup_droppedFrames
Number of frames dropped by LES due to incorrect version #

invalidLecid_droppedFrames
Number of frames dropped by LES due to invalid LECID NARP and topology requests

unknownLecid_droppedFrames
Number of frames dropped by LES due to unknown LECID ARP and FLUSH responses

invalidOpcode_droppedFrames
Number of frames dropped by LES due to invalid opcode

dupJoin_droppedFrames
Number of duplicate join requests dropped by LES because processing of the original request had not completed

incompleteSourceJoin_droppedFrames
Number of frames dropped by LES because the source LEC had not completed the JOIN phase

incompleteTargetJoin_droppedFrames
Number of frames dropped by LES because the target LEC had not completed the JOIN phase

noProxy_droppedFrames
Number of “unknown” ARP requests dropped by LES because the ELAN had no proxy LEC members

lecsWaitingForCtrlDist
Number of LECs on this ELAN waiting to be added to the LES Control Distribute VCC due to the Add Party message being delayed due to suspected ATM switch congestion.

verifyOk
Number of successful VERIFY responses.

outVerifyFails
Number of failed VERIFY responses.

inRedundancyStatus
Number of LES-BUS Redundancy Status messages received by LES.

outRedundancyStatus
Number of LES-BUS Redundancy Status messages sent by LES.

Example:

```
EXISTING LES-BUS+ statistics display les lec-les lecid
LECID [0]? 1
ATM Forum LEC-LES MIB Statistics:
   recvs:                                  3
   inRegReq:                               1
   inUnReg:                                0
   inLeArpUcast:                           0
   inLeArpBcast:                           1
   inLeArpResp:                            0
   inNArp:                                 0
Other Statistics:
   directedResp:                           3
   inLeArpRd:                              0
   inTopology:                             0
   inFlushResp:                            0
```

ATM Forum LES MIB Statistics:
The statistical counters for some fields generated by the **statistics display les lec-les** command map to MIB variables as follows:

```
LEC-LES DISPLAYED NAME                  MIB ENTRY
----------------------                  ---------
recvs                                    lesLecRecvs
inRegReq                                 lesLecInRegReq
inUnReg                                  lesLecInUnReg
inLeArpUcast                             lesLecInLeArpUcast
inLeArpBcast                             lesLecInLeArpBcast
inLeArpResp                              lesLecInLeArpResp
inNArp                                   lesLecInNAr
```

Other Statistics:

The following definitions are not MIB-related:

directedResp
Number of responses sent directly to LEC on Control Direct VCC

inLeArpRd
Number of ARP requests for route descriptors received from LEC

inFlushResp
Number of FLUSH responses received from LEC

inTopology
Number of topology requests received from LEC

display source [all or ip or ipx or netbios]
Displays statistical data for Source Management.

Example:

```
EXISTING LES-BUS+ statistics display source all
                              IP         IPX     NetBIOS       Total
                      ----------  ----------  ----------  ----------
   outNoRif:                  0           0           0           0
   outAre:                    0           0           0           0
   outSte:                    0           0           0           0
   outSrf:                    1           0           0           1
```

The statistical counters for the **statistics display source all** command map to MIB variables as follows:

```
TOTALS DISPLAYED NAME                MIB ENTRY
---------------------                ---------
outNoRif                             bcmBroadcastFramesDirectedNoRif
```

```
outAre                          bcmBroadcastFramesDirectedAre
outSte                          bcmBroadcastFramesDirectedSte
outSrf                          bcmBroadcastFramesDirectedSrf


IP DISPLAYED NAME               MIB ENTRY
-----------------               ---------
outNoRif                        bcmIpBroadcastFramesDirectedNoRif
outAre                          bcmIpBroadcastFramesDirectedAre
outSte                          bcmIpBroadcastFramesDirectedSte
outSrf                          bcmIpBroadcastFramesDirectedSrf

IPX DISPLAYED NAME              MIB ENTRY
------------------              ---------
outNoRif                        bcmIpxBroadcastFramesDirectedNoRif
outAre                          bcmIpxBroadcastFramesDirectedAre
outSte                          bcmIpxBroadcastFramesDirectedSte
outSrf                          bcmIpxBroadcastFramesDirectedSrf

NetBIOS DISPLAYED NAME          MIB ENTRY
----------------------          ---------
outNoRif                        bcmNbBroadcastFramesDirectedNoRif
outAre                          bcmNbBroadcastFramesDirectedAre
outSte                          bcmNbBroadcastFramesDirectedSte
outSrf                          bcmNbBroadcastFramesDirectedSrf
```

Stop

Use the **stop** command to stop the operation of a LES-BUS.

Syntax:

stop

Example:

```
EXISTING LES-BUS 'losangeles'+stop
Are you sure you want to stop this LES/BUS? [No]:
LES/BUS:'losangeles':not stopped
```

Takeover

Use the **takeover** command at a Primary LES-BUS to request a takeover from an active Backup LES-BUS. In the event that a Primary LES/BUS is currently yielding to an active Backup LES/BUS in a Peer Redundancy configuration, you may wish to use this command at the Primary LES/BUS console to send a takeover request to the Backup LES/BUS. Upon receipt of this request, the Backup LES/BUS terminates all LEC's and yields to the Primary LES/BUS.

Syntax:

takeover

Example:

```
EXISTING LES-BUS 't1'+takeover

Warning: If you choose to send a Takeover request to the active
Backup LES/BUS, the Backup LES/BUS will terminate all LE Clients.
This Primary LES/BUS will then be able to accept new LE Clients.
Are you sure you want to send a Takeover request? [No]: yes
LES/BUS: 'e1':Takeover Request sent to Backup LES/BUS.
EXISTING LES-BUS 't1'+
```

Terminate

Use the **terminate** command to terminate a specific LE Client from the currently operating LES-BUS.

Note: The LE Client may subsequently rejoin this ELAN or another ELAN.

LE Services monitoring commands

Syntax:

terminate atm *atm-address*

lecid *lecid*

mac *mac-address*

route-descriptor *route-descriptor*

Example:

```
EXISTING LES-BUS 'losangeles'+terminate lecid
LECID of LEC to Terminate []? 0001
The following LEC was found based on given criteria:
LEC ID:                   0x0001
   LEC ATM Address:       39999999999999000099993101100005AF972A000
   Proxy:                 Yes
   LEC State at LES:      OPERATIONAL
   LEC State at BUS:      OPERATIONAL
   MAC Address in Join Req: none
   # ATM Address Mappings:  1
   # MAC Address Mappings:  5
   # RD Mappings:           1

If you choose to TERMINATE this LEC, it may rejoin
this ELAN, or another ELAN.
Are you sure you want to terminate this LEC? [No]: no
LEC not terminated.
```

Monitoring Commands for LECS

You can create, delete, or restart an operating LECS and modify certain operating parameters of the LECS. (These changes are lost on the next restart.) You can also search through the databases of the LECS or enter into the subenvironments of the LECS console.

Enter the following commands at the `LECS console+` prompt:

Table 62. LECS Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Access-control	Provides ATM address screening for security at the LECS.
Create	Creates a LECS from its configuration data (the configuration data must already exist).
Database-synchronization	Enters the LECS database synchronization console environment.
Delete	Deletes the operating LECS.
Elans	Enters the LECS ELANs Console Environment.
List	Displays the parameters of the operating LECS.
Memory	Resets the short-term memory of the LECS.
Policies	Enters the LECS Policies Console Environment.
Restart	Restarts the LECS
Search	Searches the databases of the LECS.
Set	Modifies an operating parameter of the LECS.
Statistics	Resets or displays values of LECS counters.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Access-control

Use the **access-control** command to enter the LECS Access Control monitoring environment. These commands allow you to create a list of previously configured ATM address prefixes (1 - 20 octets) which are not allowed access to the LECS configuration database. All LECS connection attempts and configuration requests from matching ATM addresses are rejected. You can also delete and display access controls and associated statistics.

Note: To add an ATM address prefix to the list of configured prefixes, use the **access-control** command from `t 6`. See "Configuration Commands for the Access Control of a LECS" on page 380.

Syntax:

access-control

Example:

```
LECS console+ access-control
Access-Control console
LECS Access Control+
```

For additional information, see "Monitoring Commands for the Access Control of a LECS" on page 453.

Create

Use this command to create an operating LECS from the configuration data. Only one LECS is permitted on the MSS Server. This command also creates all of the policies, ELANs, and so on, for the LECS. These objects are created directly from the LECS configuration, described in "Configuration Commands for a LECS" on page 374. You can delete the LECS with the **delete** command.

Syntax:

create

Example:

```
LECS console+ create
LECS created successfully
  created all configured LECS objects
LECS console+
```

Database-synchronization

Use this command to access the `LECS Dbase Sync+` monitoring prompt from which you can begin the database synchronization process. See "LECS Database Synchronization" on page 252 for additional information.

Syntax:

database-synchronization

Example:

```
LECS console+ database-sync
LECS Dbase Sync+
```

Monitoring LECS

The following commands are available at the `LECS Dbase Sync+` prompt.

Table 63. LECS Database Synchronization Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Create	Creates an operational list of remote LECS ATM addresses from configuration data.
Delete	Deletes a LECS ATM address from participation in database synchronization.
List	Lists the database synchronization configuration.
Write	Writes the synchronized database to the remote LECSs participating in database synchronization.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Create

The **create** command creates an operational list of remote LECS ATM addresses that will participate in LECS database synchronization. This list is a subset of the addresses previously configured using database-synchronization commands in `talk 6`.

Syntax:

create

Example:

```
LECS Dbase Sync+ create
 ( 1) All enabled remote LECS ATM addresses
 ( 2) 39.99.99.99.99.99.99.00.00.99.99.45.01.40.5A.00.00.01.00
 ( 3) 39.99.99.99.99.99.99.00.00.99.99.46.01.40.5A.00.00.02.00
Remote LECS ATM Address [1]?
Created all enabled remote LECS ATM addresses
LECS Dbase Sync+
```

Delete

The **delete** command removes a remote LECS from participation in database synchronization.

Syntax:

delete

Example:

```
LECS Dbase Sync+ delete
    (1) All active remote LECS ATM addresses
    (2) 39.99.99.99.99.99.99.00.00.99.99.01.02.11.11.11.11.11.11.00
Remote LECS ATM Address:  [1] 2
Deleted remote LECS ATM address: '39.99.99.99.99.99.99.00.00.99.99.01.02.11.11.11.11.11.11.00'
LECS Dbase Sync+
```

List

The **list** command displays the list of remote LECSs configured for participation in database synchronization.

Syntax:

list

Example:

```
LECS Database Sync config> list

Remote LECS Databases to Synchronize

Remote LECS ATM Address                                          Status
=========================================================================
12.34.56.78.90.12.34.56.78.90.12.34.56.78.90.12.34.56.78.90  Synchronized

Last time LECS Database Synchronization Attempted:
  09:48:08 Friday October 30, 1998
LECS Dbase Sync+
```

Write

The **write** command writes the LECS external network configuration to the list of remote servers using database synchronization.

Syntax:

write

Example:

```
LECS Dbase Sync+ write
LECS Dbase Sync+
```

Delete

Use the **delete** command to delete an operating LECS. The LECS, along with all of its policies, ELANs, and so on, is deleted from operation. You can recreate the LECS using either the **create** or the **restart** command.

Syntax:

delete

Example:

```
LECS console+ delete
Delete LECS and all of its resources? [No]:yes
LECS deleted
LECS console+
```

Elans

Use the **elans** command to enter the LECS ELANs console environment where you can create the ELANs, LESs, and so on, known to this LECS.

Syntax:

elans

Example:

```
LECS console+ elans
LECS ELANs console
LECS ELANs+
```

List

Use this command to list the operating parameters of the LECS. Only the parameters of the LECS are listed. Individual policies, ELANs, and so on, must be accessed through submenus. The operating parameters of the LECS include its current state, an error log, the LECS ATM address, whether or not the LECS was

able to register the ATM Forum well-known address with local switch, the UNI version being used, and the configuration parameters described at “Set” on page 450.

Syntax:

list

Example:

```
LECS console+ list
Status of LECS:
ATM device number:                0
State:                            Operating normally(88)
  Time of last state change:      00.24.50.03
  Elapsed time since last change: 00.15.41.42
Error Log:                        no err (0)
Local ATM address:                39840F000000000000000000000110005A00000B00
 Well-known address:              (unable to confirm WKA registered with switch)
 UNI version:                     UNI Version 3.0
Validate best effort PCR:         No
Maximum config direct VCC reserved bandwidth:
                                  0 Kbps
Maximum number of config direct VCCs to LECS:
                                  128
Seconds before VCC declared idle: 60
Trace ATM address value:          00000000000000000000000000000000000000000000
Trace ATM address mask:           FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Auto Database Synchronization:    No
Allow Config from Remote LECS:    No
LECS console+
```

ATM device number

Number of the ATM interface over which the LECS is operating.

State The possible states of the LECS are:

Idle - The LECS exists but is not functional. This is a temporary state of the LECS; if the idle state persists, either delete or restart the LECS.

Initializing - The LECS is initializing its memory.

Activating ATM address - The LECS has initiated registration of its ATM address with the local switch but has not received confirmation of the address registration.

Activated ATM address - The LECS has received confirmation that its ATM address is registered with the local switch.

Getting UNI version - The LECS is attempting to query the local switch to determine the UNI version.

Got UNI version - The LECS has determined the UNI version being used.

ATM address deactivated - The local ATM switch has deactivated the ATM address of the LECS. If this state persists, restart the LECS.

ATM network down - The ATM interface has detected that the ATM network is not functioning correctly. LECS operation should return to normal once the ATM network is operational.

Operating normally - The normal state of the LECS.

Down due to error - An error occurred that terminated the operation of the LECS. The error log contains information explaining the error. The LECS must be restarted.

Polling status of well-known address - Certain ATM switches let you register ATM addresses that do not use the same 13–octet ATM address prefix used by the switch. For such switches, dynamic registration of the ATM Forum’s well-known LECS address is possible. During initialization, the LECS always attempts to register the well-known address with the switch. This state indicates that the LECS is currently attempting this well-known address registration.

Operating but rejecting VCCs - The **set stop** command puts the LECS into this state where it rejects all configuration direct VCCs. Use the **set start** command to return to the normal operating state.

State unknown - An error caused the state variable of the LECS to assume an unknown value. Restart or delete the LECS.

Time of last... *and* **Elapsed time since...**
These two fields indicate the last time that the LECS changed its state. The field is in the format *hh.mm.ss.dd* where *hh* is hours, *mm* is minutes, *ss* is seconds, and *dd* is hundredths of seconds. The first field lists the time that elapsed between the system initialization and the last state change, while the second field lists the time that elapsed since the last state change.

Error Log:
Describes the error that caused the LECS to enter the 'Down due to error' state. This information is used for diagnostic purposes.

Local ATM address:
ATM address of the LECS consisting of the first 13 octets from the network prefix of the local ATM switch, and appending the configured ESI and selector value. The ATM address is displayed only if it has been successfully registered with the local ATM switch.

Well-known address:
The well-known address of the LECS. The LECS attempts to register the well-known address dynamically with the ATM switch. If this dynamic registration succeeds, or if the LECS begins to receive calls to the well-known address (indicating that some other entity has registered the LECS with the local ATM switch), then this field contains the ATM Forum well-known ATM address.

UNI version:
The UNI version being used by the LECS.

Validate best effort PCR
See the **set validate** command.

Maximum config direct VCC reserved bandwidth:
See the **set reserved** command.

Maximum number of config direct VCCs to LECS:
See the **set maximum** command.

Seconds before VCC declared idle:
See the **set vcc** command.

Trace ATM address...
See the **set trace** command.

Auto Database Synchronization
See the **set auto** command. See "Set" on page 379 for more information.

Allow Config from Remote LECS
See the **set remote** command.

Memory

Use the **memory** command to clear the LECS short-term memory. The short-term memory of the LECS functions in both the redundancy and security aspects of the MSS Server LAN Emulation Service. For additional information on redundancy and

security, see “LAN Emulation Reliability” on page 248. The **memory** command can be used to reinitialize the short-term memory without restarting the LECS.

Syntax:

memory clear

Example:

```
LECS console+ memory clear
Cleared short-term memory of LECS
LECS console+
```

Policies

Use the **policies** command to enter the LECS Policies Console environment, where you can work closely with the policies guiding the LEC-to-LES assignment procedure of the LECS. You can create, delete, and display policies, and modify various policy-related counters.

Syntax:

policies

Example:

```
LECS console+ policies
LECS policies console
LECS policies+
```

Restart

Use the **restart** command to restart or create the LECS. The **restart** command stops an operating LECS, frees its resources, and reinitializes/restarts the LECS. You are prompted to either keep the current databases or to rebuild them from the static configuration data when the LECS restarts.

Syntax:

restart

Example:

```
LECS console+ restart
( 1) rebuild
( 2) retain
Retain current LECS databases or rebuild from SRAM [1]?2
LECS restarted successfully
LECS console+
```

Search

Use the **search** command to search for LES or policy value information in the LECS databases. For example, if you wanted to know to which LES the LEC with ATM address 39.00.82.48.29.10.39.38.10.AB.CD.E1.02.FA.83.29.00.00.00.1D would be assigned, use the command **search atm**, or **search atm 39.00.82.48.29.10.39.38.10.AB.CD.E1.02.FA.83.29.00.00.00.1D**

Syntax:

search atm

les

mac

name

route

Use the **search atm** command to search the LECS database of client ATM address prefixes. The output lists the longest prefix of that address found in the database, the LES associated with that prefix, and the ELAN associated with the LES.

Note: You can also search for a LES ATM address if you entered it as a non-local LES. See “Configuration Commands for ELAN Detailed Configuration” on page 384 for a description of local and non-local LESs.

Example:

```
LECS console+ search atm
ATM prefix to search for [ ]?39.00.82.48.29.10.39.38.10.AB.CD.E1.02.FA.83.29.00.00.00.1D
ATM address prefix 39.00.82.48.29.10.39.38.10.AB.CD.E1.02.FA.83.29.00.00.00.1D
  longest prefix 39.00.82.48.29.10.39.38.10.AB.CD.E1.02.FA.83.29.00.00.00.1D
      for LES address Local LES for: Accounting Ethernet Elan
          for ELAN 'Accounting Ethernet Elan'
LECS console+
```

Use the **search les** command to search for a given LES address in the LECS database of LES ATM addresses. The output lists the ELAN associated with the LES.

Example:

```
LECS console+ search les
LES to search for [ ]?39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
LES address 39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
      for ELAN 'R&D Token Ring Elan'
LECS console+
```

Use the **search mac** command to search for a given MAC address in the LECS database of client MAC addresses. You are prompted to enter whether the MAC address was entered in token-ring or Ethernet bit format (the difference being which bit is most significant). The output lists the LES associated with the MAC address and the ELAN associated with that LES.

Example:

```
LECS console+ search mac
MAC address to search for [ ]?12.34.12.34.12.35
  (  1) Ethernet bit-order
  (  2) Token ring bit-order
Bit order used by MAC address [1]?1
MAC address 12.34.12.34.12.35
    for LES address Local LES for: Accounting Ethernet Elan
      for ELAN 'Accounting Ethernet Elan'
LECS console+
```

Use the **search name** command to search for a given ELAN name in the LECS database of ELAN name policy values. The ELAN name policy value is the ELAN name used by clients in their configuration requests. The output lists the LES associated with the given ELAN name, and the ELAN associated with the LES.

Example:

```
LECS console+ search name
ELAN name to search for [ ]?R&D Elan
ELAN name 'R&D Elan'
    for LES address 39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
      for ELAN 'R&D Token Ring Elan'
LECS console+
```

Use the **search route** command to search for a route descriptor in the LECS database of client route descriptors. The output lists the LES associated with that route descriptor, and the ELAN associated with that LES.

Example:

```
LECS console+ search route
Route descriptor to search for [ ]?39.02
Route descriptor 39.02
    for LES address 39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
      for ELAN 'R&D Token Ring Elan'
LECS console+
```

Set

Use the **set** command to set various operating parameters of the LECS. These parameters take effect immediately but are not saved when you restart the LECS or the router.

Syntax:

set	maximum number of VCCs
	remote configuration
	reserved bandwidth maximum
	start accepting vccs
	stop accepting vccs
	trace ...
	validate best effort peak cell rate
	vcc idle time

Use the **set maximum** command to set the maximum number of simultaneous configuration direct VCCs permitted by the LECS. When this number is exceeded, the LECS releases all VCCs not used within the VCC idle time. VCCs that have been used within the VCC idle time are not released.

Example:

```
LECS console+ set maximum
Maximum number of simultaneous VCCs [128]?64
LECS modified
LECS console+
```

Use the **set remote** command to specify whether the LECS is allowed to have its LECS database configuration remotely overwritten by another LECS during LECS database synchronization.

Example:

```
LECS console+ set remote
Allow remote LECS configuration? [No] yes
LECS modified
LECS console+
```

Use the **set reserved** command to set the maximum reserved bandwidth on a configuration direct VCC. The LECS will not accept reserved bandwidth connections specifying a reserved bandwidth that is larger than this maximum.

Example:

```
LECS console+ set reserved
Configuration direct maximum reserved bandwidth (in Kbps) [0]?1000
LECS modified
LECS console+
```

Use the **set start** command to move the LECS into a state where it accepts VCCs (this is its normal operating state).

Example:

```
LECS console+ set start
Reject all incoming VCCs? [No]no
LECS now accepting calls
LECS console+
```

Use the **set stop** command to move the LECS into a state where it rejects all incoming VCCs. You should put the LECS in such a state before creating or deleting ELANs, policies, and so on. Otherwise, changing these other structures could result in a client issuing two identical configuration requests, but being assigned to different LESs with each request, because the modifications changed the LECS databases between configuration requests.

Example:

```
LECS console+ set stop
Reject all incoming VCCs? [Yes]:yes
LECS rejecting all VCCs
LECS console+
```

Use the **set trace** command to change the “trace mask” or the “trace value”. The trace mask and trace value are used by the LECS to determine over which VCCs packet tracing should be active. For each VCC, the LECS compares the logical AND of the trace value and the trace mask with the logical AND of the calling ATM address and the trace mask. If the resulting bit strings are identical, then the LECS should perform packet tracing on that VCC. To activate packet tracing over all VCCs, use a mask of all zeros. Packet tracing over particular VCCs is indicated by using a more specific trace mask and trace value. Packet tracing must also be enabled for the LECS subsystem through the ELS console or configuration. For additional information, refer to “Chapter 13. Using the Event Logging System (ELS)” on page 145 and “Chapter 14. Configuring and Monitoring the Event Logging System (ELS)” on page 165.

In the following examples, packet tracing is used over all VCCs with a calling party ATM address beginning with 39.84.0f.00.00.00.00.01.01.d0.d0.58.24

Example:

```
LECS console+ set trace mask
Trace ATM addr mask [ ]?ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.00.00.00.00.00.00.00
LECS modified
LECS console+
```

Example:

```
LECS console+ set trace value
Trace ATM addr value [ ]?39.84.0f.00.00.00.00.01.01.d0.d0.58.24.00.00.00.00.00.00.00
LECS modified
LECS console+
```

Use the **set validate** command to determine whether the LECS validates the peak cell rate of best-effort connections. If this parameter is true, the LECS rejects connections specifying a peak cell rate greater than the line rate of the ATM interface. Clients specifying such a peak cell rate expect that they may use more bandwidth than is available *which can adversely affect network performance*. Setting this parameter to true may create interoperability problems with clients exhibiting this behavior.

Example:

```
LECS console+ set validate
Validate best effort peak cell rate? [No]:yes
LECS modified
LECS console+
```

Use the **set vcc** command to set the VCC idle time of the LECS.

Example:

```
LECS console+ set vcc
Time (in seconds) before a VCC is declared idle [60]?30
LECS modified
LECS console+
```

Statistics

Use the **statistics** command to reset or to display many of the LECS counters.

Syntax:

statistics clear
list

Use the **statistics clear** command to reset the counters of the LECS.

Example:

```
LECS console+ statistics clear
LECS statistics cleared
LECS console+
```

Use the **statistics list** command to display the counters of the LECS.

Example:

```
LECS console+ statistics list
LECS has:
     13 ELAN(s)
     6 policy(ies) at 6 priority(ies)
LECS has 0 configure direct VCCs
     has accepted 434 VCCs and rejected 4 VCCs
     0 VCCs have been dropped by LECS, 434 dropped by caller
     has exceeded its maximum number of VCCs 0 times
LECS discarded frames: 16
LECS responses by status (zero responses if status not displayed)

     Success( 0) : 512
     Invalid request parameters( 2) : 8
     Invalid REQESTOR-ID( 8) : 4
     Invalid LAN Destination( 9) : 12
     Invalid ATM Address(10) : 4
     LE_CONFIGURE Error(21) : 12
     LECS Database Sync VCCs refused:  0
LECS console+
```

LECS has:
This is a two-line description of counters for the number of ELANs, policies, and policy priority levels at the LECS. These counters are not reset with the **statistics clear** command.

LECS has 0 configure direct VCCs
Describes counters on the VCC use of the LECS. The counter for the current number of VCCs will not be reset by the **statistics clear** command, but the other counters will.

LECS discarded frames:
Shows the number of frames that have been discarded by the LECS.

LECS responses by status ...
Describes counters for the number of responses sent by the LECS with various status values. For each possible status there is a counter. The counter value is displayed only if it is non-zero.

LECS Database Sync VCCs refused
Shows the number of times a remote LECS has attempted to overwrite the

configuration of this LECS using the database synchronization process while this LECS was configured to not allow remote configuration.

Monitoring Commands for the Access Control of a LECS

Use the **access-control** command to monitor ATM address screening at the LECS. The following commands can be issued at the `LECS Access Control+` command prompt:

Table 64. Access Control Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Create	Dynamically adds an ATM address to the screening list.
Delete	Deletes ATM address screening.
List	Displays the ATM address screening list.
Statistics	Displays statistics associated with an ATM address from the screening list.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Create

Use the **create** command to dynamically add a previously configured ATM address prefix (1 - 20 octets) to the access control screening list.

Note: To add an ATM address prefix to the list of configured prefixes, use the **access-control** command from `t 6`. See “Configuration Commands for the Access Control of a LECS” on page 380.

Syntax:

create

Example:

```
LECS console+access
LECS Access-Control console
LECS Access Control+create
  (  1) All enbld suspect ATM addresses
  (  2) 39.99.99.99.99.99.99.00.00.99.99.01.01
Suspect ATM address choice [1]? 2
Suspect ATM address created: '39.99.99.99.99.99.99.00.00.99.99.01.01'
LECS Access Control+
```

Delete

The **delete** command deletes an address prefix for access control screening.

Syntax:

delete

List

The **list** command displays the access control screening list.

Syntax:

Monitoring Access Control of a LECS

list

Example:

```
LECS Access Control+list

Suspect ATM addresses listing....

Suspect ATM address: 39.99.99.99.99.99.99.00.00.99.99.01.01
LECS Access Control+
```

Statistics

Use the **statistics** command to display or reset the counters associated with an ATM address prefix from the access control screening list.

Syntax:

statistics clear
list

clear resets the counters associated with an ATM address prefix.

list displays the ATM address prefix statistics.

Example:

```
LECS Access Control+statistics list
  (  1) All active suspect ATM addresses
  (  2) 39.99.99.99.99.99.99.00.00.99.99.01.01
Suspect ATM address choice [1]? 2

Suspect ATM address: 39.99.99.99.99.99.99.00.00.99.99.01.01
  #times access denied to address: 0

LECS Access Control+
```

Monitoring Commands for ELANs at the LECS

The LECS ELAN monitoring environment is characterized by the `LECS ELANs+` prompt. From this environment, one can create, delete, and display the ELANs of the LECS. ELAN counters can be displayed and reset. There is also a subenvironment in which one can work with the details of the ELAN, including the LESs and policy values.

Enter commands at the `LECS ELANs+` prompt.

Table 65. ELAN Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Create	Creates an ELAN from its configuration. The configuration data must already exist.
Delete	Deletes an ELAN from the operating LECS.
List	Lists all ELANs of the LECS.
Select ELAN	Selects an ELAN to monitor in more detail.
Statistics	Clears or displays the ELAN counters.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Create

Use the **create** command to create an ELAN for the LECS from the ELAN configuration data. The configuration data must already exist in static memory. For information on entering ELAN configuration data, see “Chapter 24. Using LAN Emulation Services” on page 349. Creating the ELAN results in the creation of all LESs, TLVs, and policy values for that ELAN. If you select the `All enabled ELANs` choice, then all ELANs enabled in the static configuration are created.

Syntax:

create

Example:

```
LECS ELANs+ create
 (  1) All enabled ELANs
 (  2) Accounting Ethernet Elan
 (  3) Finance Ethernet Elan
 (  4) R&D Token Ring Elan
Choice of ELAN [1]? 2
ELAN created 'Accounting Ethernet Elan'
Created TLVs for ELAN 'Accounting Ethernet Elan'
Created LESs for ELAN 'Accounting Ethernet Elan'
```

Delete

Use the **delete** command to delete an ELAN from the LECS. The LESs, TLVs, and policy values of that ELAN are also deleted. You are prompted for the ELAN to delete. If you select the ‘All Active ELANs’ choice, then all ELANs of the LECS are deleted.

Syntax:

delete

Example:

```
LECS ELANs+ delete
 ( 1) All active ELANs
 ( 2) Finance Ethernet Elan
 ( 3) R&D Token Ring Elan
 ( 4) Accounting
 ( 5) < CANCEL >
Ethernet Elan Choice of ELAN [1]? 2
Deleted ELAN 'Finance Ethernet Elan'
```

List

Use the **list** command to display a summary of the ELANs on the operating LECS.

Syntax:

list

Example:

```
LECS ELANs+ list

ELAN listing...

Type         MFS   ELAN name
============ ===== ================================
  TokenRing  4544 'R&D Token Ring Elan'
   Ethernet  1516 'Accounting Ethernet Elan'
```

Select

Use the **select** command to enter into the LECS ELAN Details monitoring environment. In this environment, you work more closely with a particular ELAN. The monitoring of LESs, TLVs, and policy values is performed in this environment. You will be prompted to select an ELAN.

Syntax:

select

Example:

```
LECS ELANs+ select
 (  1) R&D Token Ring Elan
 (  2) Accounting Ethernet Elan
 (  3) Finance Ethernet Elan
Choice of ELAN [1]? 2
ELAN 'Accounting Ethernet Elan' selected for detailed console
ELAN 'Accounting Ethernet Elan' selected+
```

Statistics

Use the **statistics** command to display or reset the counters associated with each ELAN.

Syntax:

statistics clear
list

clear resets the counters associated with an ELAN. You can clear the counters for all ELANs, or for a selected ELAN.

Example:

```
LECS ELANs+ statistics clear
 (  1) All active ELANs
 (  2) R&D Token Ring Elan
 (  3) Accounting Ethernet Elan
 (  4) Finance Ethernet Elan
 (  5) < CANCEL >
Choice of ELAN [1]? 2
Cleared stats of 1 ELANs
```

list displays the ELAN counters. You can display the counters for all ELANs or for a selected ELAN.

Example:

```
LECS ELANs+ statistics list
 (  1) All active ELANs
 (  2) R&D Token Ring Elan
 (  3) Accounting Ethernet Elan
 (  4) Finance Ethernet Elan
Choice of ELAN [1]? 3

Type         MFS   ELAN name
============ ===== ================================
   Ethernet  1516 'Accounting Ethernet Elan'
 # TLVs: 0
 # bytes in TLV data: 0
 # LES ATM addresses: 1
```

Where:

 # TLVs
is the number of TLVs which will be returned to clients assigned to this ELAN.

 # bytes in TLV data
is the total size of the TLV information which will be returned to clients assigned to this ELAN.

 # LES ATM addresses
is the number of LESs currently serving this ELAN.

Monitoring Commands for ELAN Details at the LECS

The LECS ELAN Details Console environment is characterized by the `ELAN 'elan_name' selected+` prompt, where *elan_name* is the name of the ELAN with which you are currently working. In this environment, you can modify the operational characteristics of the selected ELAN. Objects associated with the ELAN are also monitored and controlled in this environment. Such objects include:

- LESs
- TLVs
- Policy values

Enter commands at the `ELAN 'elan_name' selected+` prompt for the selected ELAN.

Table 66. ELAN Details Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
LESs	Monitor and control the LESs for this ELAN.
List	Display a summary of the ELAN.
Policy	Monitor and control the policy values assigned to any LES for this ELAN.
Set	Change the ELAN name, maximum frame size, or type of the ELAN.
ELAN-tlv	Manages TLVs associated with the selected ELAN.
LEC-tlv	Allows TLVs to be associated with an ELAN policy that is identified by ATM address, MAC address, route descriptor, or ELAN name.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

LES

Use the **les** command to monitor and control the LES ATM addresses that represent the LESs serving this ELAN. Note that no monitoring or control of the actual LES or BUS occurs. This command monitors and controls only the LES ATM address information that is returned to clients.

Syntax:

les create
delete
list
set . . .
statistics . . .

create Use the **les create** command to create LES ATM address information from

the configuration. Note that configuration data must already exist (refer to “Chapter 24. Using LAN Emulation Services” on page 349). You will be prompted to select the LES ATM address to create. Creation of this address information also creates all policy value information associated with that LES. If you select the ‘All enabled LESs’ choice, then all LESs that are enabled in static memory for this ELAN will be created.

Example:

```
ELAN 'R&D Token Ring Elan' selected+ les create
 ( 1) All enabled LESs
 ( 2) 39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
 ( 3) Local LES for: R&D Token Ring Elan
Choice of LES [1]? 3
LES created: Local LES for: R&D Token Ring Elan
Created all values for LES Local LES for: R&D Token Ring Elan
```

delete Use the **les delete** command to delete a LES ATM address from the LECS. The policy value information associated with that LES is also deleted. You must select the LES ATM address to delete. If you select the ‘All active LESs’ choice, then all LESs associated with this ELAN will be deleted.

Example:

```
ELAN 'R&D Token Ring Elan' selected+ les delete
 (  1) All active LESs
 (  2) 39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
 (  3) Local LES for: R&D Token Ring Elan
 (  4) < CANCEL >
Choice of LES [1]? 3
LES deleted: Local LES for: R&D Token Ring Elan
```

list Use the **les list** command to display the LES ATM address information associated with the selected ELAN.

Example:

```
ELAN 'R&D Token Ring Elan' selected+ les l
Primary ATM address:
39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
bckup ATM address: (no backup provided)
Primary ATM address: Local LES for: R&D Token Ring Elan
bckup ATM address: (no backup provided)
```

set *primary/backup*

Use the **les set** command to change the ATM address of primary or backup LES. You must select the LES ATM address information to modify. Refer to “Chapter 24. Using LAN Emulation Services” on page 349 for an explanation of a primary and backup LES ATM addresses.

Example:

```
ELAN 'R&D Token Ring Elan' selected+ les set primary
 (  1) 39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
 (  2) Local LES for: R&D Token Ring Elan
Choice of LES [1]?
 (  1) Local
 (  2) Remote
Primary LES is [2]?
If primary LES is remote, enter ATM address

[39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03]?
39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.05
Primary LES ATM address modified
```

statistics [clear or list]

Use the **les statistics** command to display or reset the counters associated with LESs.

clear Use the **les statistics clear** command to reset the counters of the LESs. You can reset the counters for all of the LESs, or a selected LES.

Example:

```
ELAN 'R&D Token Ring Elan' selected+ les statistics clear
 (  1) All active LESs
 (  2) 39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.05
 (  3) Local LES for: R&D Token Ring Elan
 (  4) < CANCEL >
Choice of LES [1]? 2
Cleared stats of 1 LESs
```

list Use the **les statistics list** command to display the various counters associated with each LES. You can display the counters of all LESs or a selected LES.

Example:

```
ELAN 'R&D Token Ring Elan' selected+ les statistics list
 (  1) All active LESs
 (  2) 39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.05
 (  3) Local LES for: R&D Token Ring Elan
Choice of LES [1]? 2

Primary ATM address:
39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.05
# ATM prefixes:             5  # MAC addresses:            6
# Route descriptors:        4  # Lan types:                1
# Packet sizes:             2  # ELAN names:               4
# LECs assigned to primary LES address: 0
# LECs assigned to backup LES address:  0
# LECs assigned by local check:  0
```

Note:

- The first six counters are the number of policy values in the LECS database that are associated with this LES. There is one counter for each type of policy value, and these counters are not reset with the les statistics clear command.
- The `# LECs assigned to primary LES address` field indicates the number of clients that have been given the LES ATM address information of this primary LES. This counter records the assignment only if the primary LES ATM address is a non-local LES.
- The `# LECs assigned to backup LES address` field indicates the number of clients that have been given the LES ATM address information of this backup LES. This counter records the assignment only if the backup LES ATM address is a non-local LES.
- The `# LECs assigned by local check` field indicates the number of clients that have been given LES ATM address information obtained by searching the LES-BUSs local to this MSS Server. After the LECS decides to which LES the client belongs, it queries the LES-BUSs on the MSS Server for the ATM address of an active LES for this ELAN. If there is a local LES-BUS serving this ELAN, either as a primary or backup, then the LECS obtains the definitive LES serving the ELAN. Otherwise, the LECS must use its heuristic redundancy algorithm.

List

Use this command to display a summary of the selected ELAN, including its name, maximum frame size, and type.

Syntax:

list

Example:

Monitoring ELAN Details at the LECS

```
ELAN 'R&D Token Ring Elan' selected+ list

ELAN name:      'R&D Token Ring Elan'
ELAN type:      TokenRing
Max frame size: 4544
```

Policy

Use this command to create, delete, or display the policy values assigned to LESs for this ELAN.

Syntax:

policy create *pv_type*

delete *pv_type*

list *pv_type*

create Use the **policy create** command to create an active binding between a policy value and a LES. The policy values must already exist in the static configuration (see “Chapter 24. Using LAN Emulation Services” on page 349). Policy values are used to assign requesting clients to specific LESs. You will be prompted to select the policy value to create. If you choose the ‘All enabled values’ option, then all policy values of that type that exist in the static configuration will be created.

Pv_type is one of:

- ESI/SEL of ATM address
- FRAME size
- MAC address
- NAME of ELAN
- PREFIX of ATM address
- ROUTE descriptor
- TYPE of ELAN

Example:

```
ELAN 'R&D Token Ring Elan' selected+ policy create mac
 (  1) All enabled MAC values
 (  2) 29.29.29.93.92.01 to
39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
 (  3) 29.29.29.93.92.02 to
39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
 (  4) 29.29.29.93.92.03 to
39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
 (  5) 29.29.29.93.92.04 to
39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
 (  6) 29.29.29.93.92.05 to
39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
 (  7) 29.29.29.93.92.06 to
39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
MAC address [1]? 4
MAC address value created:
29.29.29.93.92.03 to 39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
```

delete Use this command to delete active policy values. You will be prompted for the policy value to delete. If you select the ‘All active values’ option, then all policy values of that type will be deleted.

Pv_type is one of:

- ESI/SEL of ATM address
- FRAME size
- MAC address

- NAME of ELAN
- PREFIX of ATM address
- ROUTE descriptor
- Type of ELAN

Example:

```
ELAN 'R&D Token Ring Elan' selected+ policy delete route
 (  1) All active route descriptor values
 (  2) 39.92 to
39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
 (  3) 39.93 to
39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
 (  4) 39.02 to
39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
 (  5) 39.03 to
39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
Route descriptor [1]? 4
Deleted route descriptor value:
39.02 to 39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
```

list Use this command to list the active policy values for this ELAN.

Pv_type is one of:

- ESI/SEL of ATM address
- FRAME size
- MAC address
- NAME of ELAN
- PREFIX of ATM address
- ROUTE descriptor
- TYPE of ELAN

Example:

```
ELAN 'R&D Token Ring Elan' selected+ policy list name

ELAN name => LES
================================================================================
 'R&D Elan'
 => 39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
 'R&D'
  => 39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
  'R & D'
  => 39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
  'R&D Token Ring Elan'
  => 39.99.99.99.99.99.99.01.01.01.02.02.02.84.92.84.92.83.83.03
```

Set

Use this command to change the ELAN name, maximum frame size, or type. These modifications do not affect the static configuration and are lost on a restart of the LECS or router.

Syntax: set frame

name

type

frame Use this command to change the maximum frame size of the selected ELAN.

Example:

```
ELAN 'R&D Token Ring Elan' selected+ set frame
(  1) 1516
(  2) 4544
(  3) 9234
(  4) 18190
Maximum frame size of ELAN [2]? 3
Attempting to modify max frame size...ELAN modified
```

name Use this command to change the name of the selected ELAN.

Example:

```
ELAN 'R&D Token Ring Elan' selected+ set name
Name of ELAN [R&D Token Ring Elan]? R&D Token Ring Elan 1
Attempting to modify ELAN name...ELAN modified
```

type Use this command to change the type of the selected ELAN.

Example:

```
ELAN 'R&D Token Ring Elan 1' selected+ set type
(  1) Ethernet
(  2) TokenRing
Type of ELAN [2]? 2
Attempting to modify ELAN type...ELAN modified
```

ELAN-TLV

Type/length/values (TLVs) are optional configuration parameters that can be returned to all clients assigned to the selected ELAN. ELAN-TLVs are TLVs that should be returned to all clients assigned to the selected ELAN.

See “LEC-TLV” on page 394 for information about configuring TLVs that are returned to a particular LEC assigned to the selected ELAN.

Table 67. Selected ELAN-TLV Monitoring Commands Summary

Command	Function
Add	Adds a TLV to the selected ELAN.
Disable	Disables a TLV for the selected ELAN.
Enable	Enables a TLV for the selected ELAN.
List	List the configured ELAN-TLVs.
Remove	Removes a TLV from the selected ELAN.

Use the **elan-tlv add** command to add the specified TLVs of the selected ELAN. You can use the following parameters with the **elan-tlv** command:

- ATM Forum TLVs
- IBM TLVs
- MPS (MPOA Server) TLVs
- MPC (MPOA Client) TLVs
- User Defined TLVs

elan-tlv add

Syntax: elan-tlv add *atm*.

Choose from :

- C7 : Control timeout
- C10:Maximum unknown frame count
- C11:Maximum unknown frame time
- C12:VCC timeout period
- C13:Maximum retry count
- C17:Aging time
- C18:Forward delay time
- C20:Expected LE_ARP response time
- C21:Flush timeout
- C22:Path switching delay
- C23:Local segment ID
- C24:Mcast send VCC type
- C25:Mcast send VCC avg rate

- C26:Mcast send VCC peak rate
- C28:Connection complete timer
- C31: ELAN Identifier
- C35: Preferred LES

Syntax: elan-tlv add *ibm*.

Choose from :

- I4: Validate PCR of DDVCCs
- I5: Maximum Reserved Bandwidth of DDVCCs
- I6: Requested DDVCC Type
- I7: Requested DDVCC Peak Cell Rate
- I8: Requested DDVCC Avg Cell Rate
- I9: Requested DDVCC QoS Class
- I10: Negotiate Cell Rates on DDVCCs
- I11: Maximum burst size of DDVCCs

Syntax: elan-tlv add *mps*.

Choose from :

- p1: Keep-Alive Time
- p2: Keep-Alive Lifetime
- p3: InternetWork-layer Protocols
- p4: Initial Retry Time
- p5: Retry Time Maximum
- p6: Give-up Time
- p7: Hold Down Time

Syntax: elan-tlv add *mpc*.

Choose from :

- p1: SC-Setup Frame Count
- p2: SC-Setup Frame Time
- p3: Flow-detection Protocols
- p4: Initial Retry Time
- p5: Retry Time Maximum
- p6: Hold Down Time

Syntax: elan-tlv add *user*.

You can define and add their own TLVs.

Example:

```
Selected ELAN 'joe'> elan-tlvs add user
Type of TLV (in hex) [0]
Description of TLV user-tlv example
Length of TLV [4]
Value of TLV (in hex) [] cabacaba
TLV added: user-tlv example
Selection "Flush timeout TLV add" Complete
Selected ELAN 'joe'>
```

disable

Use the **elan-tlv disable** command to disable a TLV in the static configuration. The TLV will not become active on the next router restart. You are prompted to select the TLV to disable.

Syntax: elan-tlv disable

Example:

```
Selected ELAN 'lgrove001'> elan-tlv disable
TLV choice:
        (1) All
        (2) T x00A03E01 C7 : Control timeout (sec)       L 2   V 120
        (3) T x00A03E02 C10: Maxmm unknown frame count   L 2   V 1
        (4) T x00A03E03 C11: Mxmm unknwn frm time (sec)  L 2   V 1
        (5) T x00A03E04 C12: VCC timeout period (sec)    L 4   V 1200
        (6) T x00A03E05 C13: Maximum retry count         L 2   V 1
        (7) T x00A03E06 C17: Aging time (sec)            L 4   V 300
        (8) T x00A03E07 C18: Forward delay time (sec)    L 2   V 15
        (9) T x00A03E08 C20: Expctd LE_ARP rspnse (sec)  L 2   V 1
        (10) T x00A03E09 C21: Flush timeout (sec)         L 2   V 4
        (11) T x00A03E0A C22: Path switching delay (sec)  L 2   V 6
        (12) T x00A03E0B C23: Local segment ID (hex)      L 2   V ff:00
        (13) T x00A03E0C C24: Mcst send VCC type (dec)    L 2   V 2
        (14) T x00A03E0D C25: Mcst snd VCC avrg rt (cps)  L 4   V 0
        (15) T x00A03E0E C26: Mcst snd VCC peak rt (cps)  L 4   V 0
        (16) T x00A03E0F C28: Cnnctn complete time (sec)  L 2   V 4

Enter Selection:  [1]? 1
Disabled all TLVs for ELAN 'lgrove001'
Selection "TLV disable" Complete
Selected ELAN 'lgrove001'>
```

enable

Use the **elan-tlv enable** command to enable a TLV in the static configuration. The selected TLV will become active on the next router restart. You are prompted to select the TLV to enable.

list

Use the **elan-tlv list** command to list all TLVs of the selected ELAN.

```
Selected ELAN 'lgrove001'> elan-tlv list
TLVs for ELAN 'lgrove001'

Enabled  TLV
=======  ============================================================
    Yes  Type: x00A03E01 'C7 : Control timeout (sec)'
    Len: 2 Value: 120
    Yes  Type: x00A03E02 'C10: Maxmm unknown frame count'
    Len: 2 Value: 1
    Yes  Type: x00A03E03 'C11: Mxmm unknwn frm time (sec)'
    Len: 2 Value: 1
    Yes  Type: x00A03E04 'C12: VCC timeout period (sec)'
    Len: 4 Value: 1200
    Yes  Type: x00A03E05 'C13: Maximum retry count'
    Len: 2 Value: 1
    Yes  Type: x00A03E06 'C17: Aging time (sec)'
    Len: 4 Value: 300
    Yes  Type: x00A03E07 'C18: Forward delay time (sec)'
    Len: 2 Value: 15
    Yes  Type: x00A03E08 'C20: Expctd LE_ARP rspnse (sec)'
    Len: 2 Value: 1
    Yes  Type: x00A03E09 'C21: Flush timeout (sec)'
    Len: 2 Value: 4
    Yes  Type: x00A03E0A 'C22: Path switching delay (sec)'
    Len: 2 Value: 6
    Yes  Type: x00A03E0B 'C23: Local segment ID (hex)'
    Len: 2 Value: ff:00
    Yes  Type: x00A03E0C 'C24: Mcst send VCC type (dec)'
    Len: 2 Value: 2
    Yes  Type: x00A03E0D 'C25: Mcst snd VCC avrg rt (cps)'
    Len: 4 Value: 0
    Yes  Type: x00A03E0E 'C26: Mcst snd VCC peak rt (cps)'
```

```
 Len: 4 Value: 0
 Yes  Type: x00A03E0F 'C28: Cnnctn complete time (sec)'
 Len: 2 Value: 4
Selected ELAN 'lgrove001'>
```

remove

Use the **elan-tlv remove** command to remove a TLV from the static configuration of the selected ELAN. You are prompted to select the TLV to remove.

Example:

```
Selected ELAN 'lgrove001'> elan-tlv remove
TLV Choice:
 (1) All
 (2) T x00A03E01 C7 : Control timeout (sec)       L 2   V 120
 (3) T x00A03E01 C7 : Control timeout (sec)       L 2   V 100
 (4) T x00A03E02 C10: Maxmm unknown frame count   L 2   V 1
 (5) T x00A03E03 C11: Mxmm unknwn frm time (sec)  L 2   V 1
 (6) T x00A03E04 C12: VCC timeout period (sec)    L 4   V 1200
 (7) T x00A03E05 C13: Maximum retry count         L 2   V 1
 (8) T x00A03E06 C17: Aging time (sec)            L 4   V 300
 (9) T x00A03E07 C18: Forward delay time (sec)    L 2   V 15
 (10) T x00A03E08 C20: Expctd LE_ARP rspnse (sec)  L 2   V 1
 (11) T x00A03E09 C21: Flush timeout (sec)         L 2   V 4
 (12) T x00A03E0A C22: Path switching delay (sec)  L 2   V 6
 (13) T x00A03E0B C23: Local segment ID (hex)      L 2   V ff:00
 (14) T x00A03E0C C24: Mcst send VCC type (dec)    L 2   V 2
 (15) T x00A03E0C C24: Mcst send VCC type (dec)    L 2   V 0
 (16) T x00A03E0D C25: Mcst snd VCC avrg rt (cps)  L 4   V 0
 (17) T x00A03E0E C26: Mcst snd VCC peak rt (cps)  L 4   V 0
 (18) T x00A03E0F C28: Cnnctn complete time (sec)  L 2   V 4
 Enter Selection:  [1]?2

 TLV deleted: T x00A03E01 C7 : Control timeout (sec)       L 2   V 120
 Selection "TLV remove" Complete
 Selected ELAN 'lgrove001'>
```

LEC-TLV

Type/length/values (TLVs) can be associated with an individual LEC or group of LECs assigned to the selected ELAN. The set of LECs effected is determined by one of the configured ELAN policy values. For example, LEC-TLVs can be used to distinguish LECs with different QoS, giving their traffic different priority or bandwidth than other LECs associated with the same ELAN.

See “ELAN-TLV” on page 390 for information about configuring TLVs to be associated with all LECs assigned to the selected ELAN.

The following table shows the different identifiers you can use to select the individual LECs associated with a particular policy.

Table 68. Selected LEC-TLV Identifiers Summary

Identifier	Purpose
ESI/SEL of ATM address	Uses an ESI/Selector of ATM address policy to identify the LECs to be associated with the TLV.
MAC address	Uses a MAC address policy to identify the LECs to be associated with the TLV.
Name of ELAN	Uses an ELAN name policy to identify the LECs to be associated with the TLV.
PREFIX of ATM address	Uses an ATM address prefix policy to identify the LECs to be associated with the TLV.
Route Descriptor	Uses a route descriptor policy to identify the LECs to be associated with the TLV.

After a policy is chosen, use the following commands to select and monitor TLVs to be returned to all LECs assigned by the selected policy.

Monitoring ELAN Details at the LECS

Table 69. Selected LEC-TLV Command Summary

Command	Function
Add	Adds a TLV to the selected ELAN policy.
Disable	Disables a TLV for the selected ELAN policy.
Enable	Enables a TLV for the selected ELAN policy.
List	Lists TLVs for the selected ELAN policy.
Remove	Removes a TLV from the selected ELAN policy.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Example:

```
 Selected ELAN 'lgrove01'>policy list prefix

ATM prefixes for ELAN 'lgrove01'
Enabled  Value  =>  LES
=======  ========================================
     No  55
            => Local LES for: lgrove01
     No  25
            => Local LES for: lgrove01
Selected ELAN 'lgrove01'>lec-tlv prefix
  (  1) 55
  (  2) 25
ATM prefix [1]?
Policy Value '55' selected for detailed TLV configuration
Tlvs for '55' selected+add ibm i4
I4: Validate peak cell rate of Best Effort DDVCCs? [No]: yes
TLV added: I4: Vldt PCR of Bst Effrt DDVCC
Tlvs for '55' selected+list
Enabled  TLV
=======  ======================================================
    Yes  Type: x10005A04 'I4: Vldt PCR of Bst Effrt DDVCC'
         Len: 4 Value: 1

Tlvs for '55' selected+
```

Monitoring Commands for LECS Policies

The LECS Policy monitoring environment is characterized by the `LECS policies+` prompt. From this environment, you can monitor and control the policies guiding the LEC-to-LES assignment procedure of the LECS. You can create, delete, or display policies, and display or reset certain counters associated with the policies.

Enter commands at the `LECS policies+` prompt which you can get to from the `LECS console+` prompt for the specified LES-BUS.

Table 70. LECS Policies Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Create	Creates a policy for the operating LECS (the policy must already exist in the configuration data).
Delete	Deletes a policy for the operating LECS.
List	Lists the policies for the operating LECS.
Statistics	Displays or resets certain counters associated with the LECS policies.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Create

Use the **create** command to create a policy from the configuration data. Note that the policy must exist in the static configuration before it can be created. You are prompted for the policy that you wish to create. If you specify the `All enbld pols` choice, then all policies that are enabled in the static configuration are created.

Syntax:

create

Example:

```
LECS policies+ create
(  1) All enbld pols
(  2) 100  byAtmAddr
(  3) 200  byMacAddr
(  4) 300  byRteDesc
(  5) 400  byElanNm
(  6) 1000 byLanType
(  7) 1100 byPktSize
Choice of policy [1]? 5
Policy created: '400  byElanNm '
LECS policies+
```

Delete

Use the **delete** command to delete a policy from the operating LECS. You will be prompted for the policy that you wish to delete. If you specify the `All active pols` choice, all policies of the LECS are deleted.

Syntax:

delete

Example:

```
LECS policies+ delete
(  1) All active pols
(  2) 100  byAtmAddr
(  3) 200  byMacAddr
(  4) 300  byRteDesc
(  5) 400  byElanNm
(  6) 1000 byLanType
(  7) 1100 byPktSize
Choice of policy [1]? 3
Deleted policy: '200  byMacAddr'
LECS policies+
```

List

Use the **list** command to list the policies of the active LES.

Syntax:

list

Example:

```
LECS policies+ list

Policy listing....

Priority:    100  Policies: byAtmAddr
Priority:    300  Policies: byRteDesc
```

```
Priority:    400  Policies: byElanNm
Priority:   1000  Policies: byLanType
Priority:   1100  Policies: byPktSize
LECS policies+
```

Statistics

Use the **statistics clear** command to reset the counters associated with the LECS policies. You can clear the statistics of all policies, or only of the policies at a certain priority level.

Syntax:

statistics clear
list

Example:

```
LECS policies+ statistics clear
(  1) All active policies
(  2) 100   byAtmAddr
(  3) 300   byRteDesc
(  4) 400   byElanNm
(  5) 1000  byLanType
(  6) 1100  byPktSize
(  7) < CANCEL >
Choice of policy [1]? 3
Cleared stats of 1 priority levels
LECS policies+
```

Use the **statistics list** command to display the counters associated with the LECS policies. You can display the counters for all policies, or only for the policies at a certain priority level.

Example:

```
LECS policies+ statistics list
(  1) All active policies
(  2) 100   byAtmAddr
(  3) 300   byRteDesc
(  4) 400   byElanNm
(  5) 1000  byLanType
(  6) 1100  byPktSize
Choice of policy [1]? 4
Priority:    400  Policies: byElanNm
#policies at this priority: 1
#times assigned by policy: 158
#times policy failed: 253

LECS policies+
```

Priority
Counters are maintained for each priority level.

#policies at this priority
This counter is not reset by the statistics clear command.

#times assigned by policy
This counts the number of times that the LECS used the policies at this priority level to assign a client to a LES.

#times policy failed
This counts the number of times that the LECS attempted to use the policies at this priority level to assign a client to a LES, but failed.

Monitoring Commands for Security for LE Service

The LES-LECS Security Interface monitoring environment is characterized by the `LES-LECS interface+` prompt. From this environment, the LES-LECS interface can be created, deleted, or restarted. Counters associated with the LES-LECS interface can be reset or displayed. The LES-LECS Security Interface is the LE Services component responsible for multiplexing configuration requests from the LESs on the MSS Server to the LECS (which may or may not be on the MSS Server). The LES-LECS interface is a required component if any of the LES-BUSs are using the security features of the MSS Server.

Enter commands at the `LES-LECS interface+` prompt. To access the prompt for monitoring, do the following:

```
+ network net#
ATM+ le-s
LE-Services Console
LE-SERVICES+ security
LES-LECS Security Interface
LES-LECS interface+
```

Table 71. Security for LE Services Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Create	Creates the LES-LECS interface for the authentication of LE client joins.
Delete	Deletes the LES-LECS interface for the authentication of LE client joins.
List	Lists the LES-LECS interface’s status and current configuration parameters.
Restart	Restarts a running LES-LECS interface.
Statistics	Clears or lists statistics of the LES-LECS interface.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Create

Use the **create** command to create the LES-LECS Interface for authentication of LE Client Joins. The LES-LECS Interface configuration must exist before it can be created (see “Configuration Commands for Security for ELANs” on page 398). By default, when an Multiprotocol Switched Services (MSS) boots up, the LES-LECS Interface is created if it is configured and enabled. The **create** command allows the LES-LECS Interface to be created without restarting the entire router.

Syntax:

create

Example:

```
LES-LECS interface+ create
LECS interface created on device 0
```

Delete

Use the **delete** command to stop an LES-LECS Interface and remove it from the active configuration. (The LES-LECS Interface definition remains in Static configuration.) If you issue the **delete** command and then want to start the LES-LECS Interface without restarting the Multiprotocol Switched Services (MSS), issue the **create** command.

Security for LE Service monitoring commands

Syntax:

delete

Example:

```
LES-LECS interface+ delete
LECS interface deleted
```

List

Use the **list** command to list the status and current configuration parameters of the LES-LECS Interface.

Syntax:

list

Example:

```
LES-LECS interface+ list
Status of LES-LECS Security Interface
  ATM Device Number:     0
  State:                 Operating normally(110)
    Time of last state change:      00.23.44.26
    Elapsed time since last change: 00.01.10.70
  Error Log:             no err(0)
  ATM address:           39999999999999000099990101100005a68001201
  UNI version            UNI Version 3.0
  Connected LECS:        47007900000000000000000000a03e00000100(local)
  VCC characteristics:
    Configuration direct VCC type:      Best Effort
    Configuration direct VCC PCR:       155000
```

Where:

State Is the operational state of the LES-LECS Interface. Possible states are:

- Idle
- Initializing
- Activating ATM address
- Activated ATM address
- Getting UNI version
- Got UNI version
- Getting list of LECSs
- Got list of LECSs
- Attempting to connect to LECS
- Failed to connect to LECS - will retry
- Operating normally
- Connection to LECS released - will retry
- ATM address deactivated
- ATM network down
- Down due to error
- State unknown!!!

Time of last state change
Is the system up time that the LES-LECS Interface entered its current state. The format is *hours.minutes.seconds.hundredths*

Elapsed time since last change
Is the amount of time since the last state change. The format is hours.minutes.seconds.hundredths

Error Log
Is the reason the LES-LECS Interface last went down. If the LES-LECS Interface has not been down since the last MSS Server restart, `no err` appears. An additional error code is contained within the parentheses.

ATM Address
Is the ATM address of the LES-LECS Interface.

Connected LECS
Is the ATM address used by the LES-LECS Interface to connect to the LECS. Following this ATM address is an indication of whether the LECS is local to this MSS Server or remote, that is, on another device.

Configuration direct VCC type
Indicates whether the LES-LECS Interface uses a best effort or reserved bandwidth VCC to the LECS.

Configuration direct VCC PCR
Indicates the peak cell rate of the configuration direct VCC to the LECS.

VCC characteristics
If VCC type is Reserved Bandwidth, the Sustained Cell Rate of the VCC in Kbps is shown.

Restart

Use the **restart** command to restart a running LES-LECS Interface.

Syntax:

restart

Example:

```
LES-LECS interface+ restart
LECS interface restarted on device 0
```

Statistics

Use the **statistics** command to clear or list all LES-LECS Interface statistics.

Syntax:

statistics clear
list

clear Sets all LES-LECS Interface statistics to zero.

Example:

```
LES-LECS interface+ statistics clear
LECS interface statistics cleared
```

list Shows all statistics for the LES-LECS Interface.

Example:

```
LES-LECS interface+ statistics list
Statistics of LES-LECS Security Interface
  # queries to local LECS:          3
  # frames transmitted:             0
  # frames received:                0
```

```
# discarded frames:               0
# VCCs released by LECS/network:  0
# failed VCC setup attempts:      0
```

Where:

 # VCCs released by LECS/network
Is the number of times Security VCC from the LES-LECS Interface to the LECS has been released. Releases due to LES-LECS Interface errors or changes in the LES-LECS Interface administrative status are not counted.

 # failed VCC setup attempts
Is the number of Security VCC call setup requests made by the LES-LECS Interface that failed for any reason.

Chapter 26. Configuring and Monitoring Quality of Service (QoS)

This chapter describes Quality of Service (QoS) configuration and operational commands for LAN and ELAN interfaces in the router. It contains the following sections:

- "Quality of Service Overview"
- "QoS Configuration Parameters" on page 474
- "Accessing the QoS Configuration Prompt" on page 478
- "Quality of Service Commands" on page 479
- "LE Client QoS Configuration Commands" on page 480
- "ATM Interface QoS Configuration Commands" on page 484
- "Accessing the QoS Monitoring Commands" on page 487
- "Quality of Service Monitoring Commands" on page 487
- "LE Client QoS Monitoring Commands" on page 488

Quality of Service Overview

The QoS feature leverages the benefits of ATM QoS capabilities for LAN Emulation Data Direct VCCs. This support is referred to as "Configurable QoS for LAN Emulation". The key attributes and the benefits of this feature are as follows:

- An LE Client makes use of configured QoS parameters for its Data Direct VCCs.
- QoS parameters can be configured for:
  - LE Client
  - Emulated LAN
  - ATM Interface
- The set of QoS parameters configured are for use with ATM Forum UNI 3.0/3.1 signaling. The parameters include the desired Peak Cell Rate, Sustained Cell Rate, QoS Class and Maximum Burst Size.
- Maximum Reserved Bandwidth per VCC can be configured to protect an LE Client from accepting/establishing VCCs whose traffic parameters it cannot support.
- The QoS Negotiation mechanism enables the participating LE Clients to be aware of each other's QoS parameters. A data-direct VCC is set up using the negotiated parameters.

Benefits of QoS

- Using QoS for the LE Client, ATM Interface, or Emulated LAN provides the following benefits for LANE Data Direct VCCs.
  - An LE Client can be configured with QoS if the QoS required by the client is different from the QoS required by other clients on the ELAN. For example, if an LE Client serves a file server, then the user may want to configure appropriate QoS parameters for all traffic to and from the file server.
  - An Emulated LAN can be configured with QoS if the user wishes to provide QoS for all traffic in that ELAN. For example, an ELAN carrying SNA traffic can be given priority by configuring QoS parameters for that ELAN.

© Copyright IBM Corp. 1996, 1998

– An ATM Interface can be configured with QoS if a user wants all LE Clients on that ATM interface to use the same set of parameters. For example, if an ATM Interface is connected at 25 Mbps, the user can configure appropriate parameters that are different from those at a 155-Mbps interface.

QoS Configuration Parameters

This section describes nine parameters that are used for QoS configuration. The following six parameters can be configured for an LE Client, ATM Interface, and an Emulated LAN:

1. max-reserved-bandwidth
2. traffic-type
3. peak-cell-rate
4. sustained-cell-rate
5. max-burst-size
6. qos-class

The following two parameters can be configured for an Emulated LAN and an LE Client:

1. *validate-pcr-of-best-effort-vccs*
2. *negotiate-qos*

The *accept-qos-parms-from-lecs* parameter can be configured only for an LE Client.

The first six parameters control the traffic characteristics of Data Direct VCCs established by the LE Client while the first parameter also applies to the calls received by the LE Client. The following characteristics are associated with all the Data Direct VCCs established by the LE Client:

- Bandwidth is not reserved for best-effort traffic.
- Traffic parameters apply to both forward and backward directions.
- When a reserved bandwidth connection is rejected due to the traffic parameters or QoS Class, the call is retried as a best-effort connection with the configured peak cell rate (cause codes on release or release-complete messages are used to determine why a VCC was released).
- When a best-effort connection is rejected due to the Peak Cell Rate (PCR), the call may be automatically retried with a lower PCR. Retries are performed under the following conditions:
  1. If the rejected PCR is greater than 100 Mbps, the call is retried with a PCR of 100 Mbps.
  2. Otherwise, if the rejected PCR is greater than 25 Mbps, the call is retried with a PCR of 25 Mbps.

Maximum Reserved Bandwidth (max-reserved-bandwidth)

The maximum reserved bandwidth acceptable for a Data Direct VCC. This parameter applies to both Data Direct VCC calls received by the LE Client and Data Direct VCC calls placed by the LE Client. For incoming calls, this parameter defines the maximum acceptable SCR for a Data Direct VCC. If SCR is not specified on the incoming call, then this parameter defines the maximum acceptable PCR for a Data Direct VCC with reserved bandwidth.

Calls received with traffic parameters specifying higher rates will be released. If SCR is specified on the incoming call, the call will not be rejected due to the PCR or Maximum Burst Size. The constraint imposed by this parameter is not applicable to BEST_EFFORT connections. For outgoing calls, this parameter sets an upper bound on the amount of reserved bandwidth that can be requested for a Data Direct VCC. Therefore the traffic-type and sustained-cell-rate parameters are dependent upon this parameter.

Valid Values:
Integer in the range 0 to the line speed of ATM device in Kbps

Default Value:
0

Traffic Type (traffic-type)

The desired traffic type for Data Direct VCCs. If QoS parameters are not negotiated, then this parameter specifies the type of calls placed by the LE Client. Otherwise, if QoS parameters are negotiated, this parameter specifies the desired type of traffic characteristics for Data Direct VCCs. When QoS parameters are negotiated, if either the source or target LEC desires a reserved bandwidth connection and both LECs support reserved bandwidth connections (that is, max-reserved-bandwidth > 0), then an attempt will be made to establish a reserved bandwidth Data Direct VCC between the two LECs. Otherwise, the Data Direct VCC will be a best-effort connection. Dependencies: max-reserved-bandwidth

Valid Values:
best_effort or reserved_bandwidth

Default:
best_effort

Peak Cell Rate (peak-cell-rate)

The desired peak cell rate for Data Direct VCCs. If QoS parameters are not negotiated, then this parameter specifies the PCR traffic parameter for Data Direct VCC calls placed by the LE Client. Otherwise, if QoS parameters are negotiated, this parameter specifies the desired PCR traffic parameter for Data Direct VCCs. The minimum of the desired PCRs of the two LECs is used for negotiated best-effort VCCs.

When a reserved bandwidth VCC is negotiated and only one of the LE Clients requests a reserved bandwidth connection, then the desired PCR of that LEC is used for the Data Direct VCC subject to the upper bound imposed by the line rate of the local ATM device. If both LECs request a reserved bandwidth connection, then the maximum of the desired PCRs of the LE Clients is used for the Data Direct VCC subject to the upper bound imposed the line rate of the local ATM device.

Valid Values:
An integer value in the range 0 to the line speed of ATM device in Kbps

Default Value:
Line speed of LEC ATM Device in Kbps.

Sustained Cell Rate (sustained-cell-rate)

The desired sustained cell rate for Data Direct VCCs. If QoS parameters are not negotiated, then this parameter specifies the SCR traffic parameter for Data Direct

VCC calls placed by the LE Client. Otherwise, if QoS parameters are negotiated, this parameter specifies the desired SCR traffic parameter for Data Direct VCCs.

When a reserved bandwidth VCC is negotiated and only one of the LE Clients requests a reserved bandwidth connection, then the desired SCR of that LEC is used for the Data Direct VCC (subject to the upper bound imposed by the max-reserved-bandwidth parameter of the other LEC). If both LECs request a reserved bandwidth connection, then the maximum of the desired SCRs of the LE Clients is used for the Data Direct VCC (subject to the upper bound imposed by the max-reserved-bandwidth parameters of both LECs). In any case (negotiation or not), if the SCR that is to be signaled equals the PCR that is to be signaled, then the call is signaled with PCR only.

Dependencies: max-reserved-bandwidth, traffic-type and peak-cell-rate. This parameter is applicable only when traffic-type is RESERVED_BANDWIDTH.

Valid Values:

An integer value in the range 0 to the minimum of max-reserved-bandwidth and peak-cell-rate, specified in Kbps

Default Value

None

Maximum Burst Size (max-burst-size)

The desired maximum burst size for Data Direct VCCs. If QoS parameters are not negotiated, then this parameter specifies the Maximum Burst Size traffic parameter for Data Direct VCC calls placed by the LE Client. Otherwise, if QoS parameters are negotiated, this parameter specifies the desired Maximum Burst Size traffic parameter for Data Direct VCCs.

When a reserved bandwidth VCC is negotiated and only one of the LE Clients requests a reserved bandwidth connection, then the desired Maximum Burst Size of that LEC is used for the Data Direct VCC. If both LECs request a reserved bandwidth connection, then the maximum of the desired Maximum Burst Sizes of the LE Clients is used for the Data Direct VCC.

In any case (negotiation or not), the Maximum Burst Size is signaled only when SCR is signaled. Although this parameter is expressed in units of cells, it is configured as an integer multiple of the Maximum Data Frame Size (specified in LEC's C3 parameter) with a lower bound of 1.

Dependencies: This parameter is applicable only when traffic-type is RESERVED_BANDWIDTH.

Valid Values:

An integer number of frames; must be greater than 0

Default:

1 frame

QoS Class (qos-class)

The desired QoS class for reserved bandwidth calls. If QoS parameters are not negotiated, then this parameter specifies the QoS Class to be used for reserved bandwidth Data Direct VCC calls placed by the LE Client. Otherwise, if QoS parameters are negotiated, this parameter specifies the QoS Class that is desired

for Data Direct VCCs. Unspecified QoS Class is always used on best-effort calls. Specified QoS Classes define objective values for ATM performance. Specified QoS Classes define objective values for ATM performance parameters such as cell loss ratio and cell transfer delay.

The UNI Specification states that:

Specified QoS Class 1
should yield performance comparable to current digital private line performance.

Specified QoS Class 2
is intended for packetized video and audio in teleconferencing and multimedia applications.

Specified QoS Class 3
is intended for interoperation of connection oriented protocols, such as Frame Relay.

Specified QoS Class 4
is intended for interoperation of connectionless protocols, such as IP or SMDS.

LECs must be able to accept calls with any of the above QoS Classes. When QoS parameters are negotiated, the configured QoS Classes of the two LECs are compared, and the QoS Class with the more stringent requirements is used.

Valid Values:
0: for Unspecified QoS Class

1: for Specified QoS Class 1

2: for Specified QoS Class 2

3: for Specified QoS Class 3

4: for Specified QoS Class 4

Default Value:
0 (Unspecified QoS Class)

Validate PCR of Best-Effort VCCs (validate-pcr-of-best-effort-vccs)

To validate Peak Cell Rate of Best-Effort VCCs. When FALSE, best-effort VCCs will be accepted without regard to the signaled forward PCR. When TRUE, best- effort VCCs will be rejected if the signaled forward PCR exceeds the line rate of the LE Client ATM device. Calls will not be rejected due to the backward PCR. The signaled backward PCR will be honored if it does not exceed the line rate; otherwise, transmissions to the caller will be at line rate.

Notes:

1. Accepting best-effort VCCs with forward PCRs that exceed the line rate can result in poor performance due to excessive retransmissions; however, rejecting these VCCs can result in interoperability problems.
2. The YES setting is useful when callers will retry with a lower PCR following call rejection due to unavailable cell rate.

Valid Values:
yes, no

Default Value:
no

Negotiate QoS (negotiate-qos)

Enable QoS parameter negotiation for Data Direct VCCs. This parameter should be enabled only when connecting to an IBM MSS LES. When this parameter is YES, the LE Client will include an IBM Traffic Parameter TLV in LE_JOIN_REQUEST and LE_ARP_RESPONSE frames sent to the LES. This TLV will include the values of max-reserved-bandwidth, traffic-type, peak-cell-rate, sustained-cell-rate, max-burst-size and qos-class. An IBM Traffic Parameter TLV may also be included in a LE_ARP_RESPONSE returned to the LE Client by the LES.

If there is no TLV in a LE_ARP_RESPONSE received by the LE Client, then the local configuration parameters must be used to setup the Data Direct VCC. If a TLV is included in a LE_ARP_RESPONSE, the LE Client must compare the contents of the TLV with the corresponding local values to determine the “negotiated” or “best” set of parameters acceptable to both parties before signalling for the Data Direct VCC.

Valid Values:
yes, no

Default Value:
no

Accept QoS Parms from LECS (accept-qos-parms-from-lecs)

This parameter gives the ability to configure an LE Client to accept/reject QoS parameters from a LECS. When this parameter is YES, the LE Client should use the QoS parameters obtained from the LE Clients in the LE_CONFIGURE_RESPONSE frames, that is, the QoS parameters from the LE Clients override the locally configured QoS parameters. If this parameter is NO then the LE Client will ignore any QoS parameters received in an LE_CONFIGURE_RESPONSE frame from the LE Clients.

Valid Values:
yes, no

Default Value:
no

Accessing the QoS Configuration Prompt

Use the **feature** command from the CONFIG process to access the Quality of Service configuration commands. Enter **feature** followed by the feature number (6) or short name (QoS). For example:

```
Config> feature qos
Configurable Quality of Service for LAN Emulation
QoS Config>
```

Once you access the `QoS Config>` prompt, you can configure the Quality of Service (QoS) of an LE Client, an Emulated LAN, or an ATM Interface. To return to the `Config>` prompt at any time, enter the **exit** command at the `QoS Config>` prompt.

Alternatively, you can configure QoS parameters for an LE Client, an Emulated LAN, or an ATM Interface by accessing the entities as follows:

- LE Client
  1. At the `Config>` prompt, enter the **network** command and the LE Client interface number.

2. At the LE Client configuration> prompt enter **qos-configuration**.

   Example:

```
config> network 3
Token Ring Forum Compliant LEC Config> qos-configuration
elan-x LEC QoS Config>
```

- ATM Interface
  1. at the Config> prompt, enter the **network** command and the ATM interface number to get you to the ATM Config> prompt.
  2. Enter the **interface** parameter to get to the ATM Interface Config> prompt.
  3. At the ATM InterfaceConfig> prompt enter **qos-configuration**.

     Example:

```
config> network 0
ATM Config> interface
ATM Interface Config> qos-configuration
ATM-I/F 0 QoS>
```

- Emulated LAN
  1. At the Config> prompt, enter the **network** command and the ATM interface number to get to the ATM Config> prompt.
  2. Enter **le-service** to get to the LE Services config> prompt.
  3. Enter **lecs** to get to the LECS config> prompt.
  4. At the LECS config> prompt enter **elans** to get to the LECS ELANS configuration> prompt.
  5. Select an ELAN by entering **select elan** *elan-x*, where *elan-x* is the ELAN you wish to configure. This will get you to the Selected ELAN '.elan-x'> prompt.
  6. At the Selected ELAN 'elan-x'> prompt, QoS parameters can be configured as TLVs. See “Configuration Commands for ELAN Detailed Configuration” on page 384 for more information.

     Example:

```
config> network 0
ATM Config> le-services
LE Services config> lecs
LECS config> elans
LECS ELANs config> select elan elan-x
Selected ELAN 'elan-x'>
```

Quality of Service Commands

This section summarizes the QoS configuration commands. Use the following commands to configure Quality of Service. Enter the commands from the QoS Config> prompt.

Table 72. Quality of Service (QoS) Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
le-client	Gets you to the LE Client QoS configuration > prompt for the selected LE client.
atm-interface	Gets you to the ATM Interface QoS configuration> prompt for the selected ATM interface.
elan (at LECS)	Gets you to the ELAN QoS configuration> prompt at LECS for configuring QoS parameters.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

LE Client QoS Configuration Commands

This section summarizes and explains the commands for configuring QoS for a specific LE Client.

Use the following commands at the `LEC QoS config>` prompt.

Table 73. LE Client Quality of Service (QoS) Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
List	Lists the current QoS configuration of the LE Client.
Set	Sets the QoS parameters of the LE Client.
Remove	Removes the QoS configuration of the LE Client.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to list the QoS configuration of this LE Client. QoS parameters are listed only if at least one has been specifically configured (see Example 1). Otherwise, no parameters are listed (see Example 2).

Syntax:

list

Example 1:

```
LEC QoS Config> list

           LE Client QoS Configuration for Data Direct VCCs
           ========================================
     (ATM interface number = 0,  LEC interface number = 3)

  Maximum Reserved Bandwidth for a Data-Direct VCC = 10000 Kbps
  Data-Direct VCC Type ........................... = Best-Effort
  Data-Direct VCC Peak Cell Rate ................. = 155000 Kbps
  Data-Direct VCC Sustained Cell Rate ............ = 155000 Kbps
  Desired QoS Class of Reserved Connections ...... = 0
  Max Burst Size of Reserved Connections    ...... = 0 frames

  Validate Peak Rate of Best-Effort connections .. = No
  Enable QoS Parameter Negotiation ............... = Yes
  Accept QoS Parameters from LECS ................ = Yes

LEC QoS Config>
```

Example 2:

```
LEC QoS Config> list

   QoS has not been configured for this LEC.
   Please use the SET option to configure QoS.

LEC QoS Config>
```

Set

Use the **set** command to specify LE Client QoS parameters.

Syntax:

set accept-qos-parms-from-lecs
all-default-values
max-burst-size
max-reserved-bandwidth
negotiate-qos
peak-cell-rate
qos-class
sustained-cell-rate
traffic-type
validate-pcr-of-best-effort-vccs

accept-qos-parms-from-lecs

Use this option to enable/disable the LE Client to accept/reject the QoS parameters received from an LECS as TLVs. See "Accept QoS Parms from LECS (accept-qos-parms-from-lecs)" on page 478 for a more detailed description of this parameter.

Valid Values:

YES, NO

Default Value:

YES

Example:

```
elan-x LEC QoS Config> se acc y
elan-x LEC QoS Config>
```

all-default-values

Use this option to set the QoS parameters to default values. In the following example the default values are also listed.

Example:

```
LEC QoS Config> set all-default-values
   Failed to locate existing QoS configuration record!
   Using a new set of default values ...
   Initializing all parameters to default values
   elan-x LEC QoS Config>  list

              LE Client QoS Configuration for Data Direct VCCs
              ========================================
         (ATM interface number = 0,  LEC interface number = 3)

     Maximum Reserved Bandwidth for a Data-Direct VCC = 0 Kbps
     Data-Direct VCC Type ........................... = Best-Effort
     Data-Direct VCC Peak Cell Rate ................. = 155000 Kbps
     Data-Direct VCC Sustained Cell Rate ............ = 155000 Kbps
     Desired QoS Class of Reserved Connections ...... = 0
     Max Burst Size of Reserved Connections    ...... = 0 frames

     Validate Peak Rate of Best-Effort connections .. = No
     Enable QoS Parameter Negotiation ............... = No
     Accept QoS Parameters from LECS ................ = Yes

  LEC QoS Config>
```

max-burst-size

Sets the desired maximum burst size in frames. See "Maximum Burst Size (max-burst-size)" on page 476 for a more detailed description of this parameter.

Valid Values:

An integer number of frames; must be greater than 0

Default:
1 frame

Example:

```
elan-x LEC QoS Config>  se ma
   Maximum Burst Size in Kbps [1]? 10000
   elan-x LEC QoS Config>
```

max-reserved-bandwidth
Use this option to set the maximum reserved bandwidth allowable per Data Direct VCC. See “Maximum Reserved Bandwidth (max-reserved-bandwidth)” on page 474 for a more detailed description of this parameter.

Valid Values:
Integer in the range 0 to the line speed of ATM device in Kbps

Default Value:
0

Example:

```
   LEC QoS Config> set max-reserved-bandwidth
   Maximum reserved bandwidth acceptable for a data-direct VCC (in Kbps) [0]? 20000
   LEC QoS Config>
```

negotiate-qos
Use this option to enable/disable the LE Client’s participation in QoS negotiation. See “Negotiate QoS (negotiate-qos)” on page 478 for a more detailed description of this parameter.

Valid Values:
YES, NO

Default Value:
NO

Example:

```
elan-x LEC QoS Config>  se neg y
elan-x LEC QoS Config>
```

peak-cell-rate
Sets the desired peak cell rate for Data Direct. See “Peak Cell Rate (peak-cell-rate)” on page 475 for a more detailed description of this parameter.

Valid Values:
An integer value in the range 0 to the line speed of ATM device in Kbps

Default Value:
Line speed of LEC ATM Device in Kbps.

Example:

```
   elan-x LEC QoS Config>  set peak-cell-rate
   Data-Direct VCC Peak Cell Rate in Kbps [1]? 25000
   elan-x LEC QoS Config>
```

qos-class
Sets the desired QoS Class for Data Direct VCCs. See “QoS Class (qos-class)” on page 476 for a more detailed description of this parameter.

Valid Values:
0: for Unspecified QoS Class

1: for Specified QoS Class 1

2: for Specified QoS Class 2

3: for Specified QoS Class 3

4: for Specified QoS Class 4

Default Value:
0 (Unspecified QoS Class)

Example:

```
elan-x LEC QoS Config>  se qos
Desired QoS Class for Data Direct VCCs [0]? 1
elan-x LEC QoS Config>
```

sustained-cell-rate
Sets the desired sustained cell rate for Data Direct VCCs. See “Sustained Cell Rate (sustained-cell-rate)” on page 475 for a more detailed description of this parameter.

Valid Values:
An integer value in the range 0 to the minimum of max-reserved-bandwidth and peak-cell-rate, specified in Kbps

Default Value
None

Example:

```
elan-x LEC QoS Config>  se sus
Data-Direct VCC Sustained Cell Rate in Kbps [1]? 10000
elan-x LEC QoS Config>
```

traffic-type
Sets the desired traffic for Data Direct VCCs. See “Traffic Type (traffic-type)” on page 475 for a more detailed description of this parameter.

Valid Values:
BEST_EFFORT or RESERVED_BANDWIDTH

Default:
BEST EFFORT.

Example:

```
elan-x LEC QoS Config> set traffic-type
  Choose from:
     (0): Best-Effort
     (1): Reserved-Bandwidth
Data Direct VCC Type [0]? 1
NOTE: Peak Cell Rate has been reset to 1
      Sustained Cell Rate has been reset to 1
      Max Reserved Bandwidth has been reset to 1
      Please configure appropriate values.
elan-x LEC QoS Config>
```

validate-pcr-of-best-effort-vccs
Use this option to enable/disable validation of the Peak Cell Rate traffic parameter of the Data Direct VCC calls received by this LE Client. See “Validate PCR of Best-Effort VCCs (validate-pcr-of-best-effort-vccs)” on page 477 for a more detailed description of this parameter.

Valid Values:
YES, NO

Default Value:
NO

Example:

```
elan-x LEC QoS Config>  se val y
elan-x LEC QoS Config>
```

Remove

Use the **remove** command to remove the QoS configuration of this LE Client.

Syntax:

remove

Example:

```
elan-x LEC QoS Config>  remove
WARNING: This option deletes the QoS configuration.
         To re-configure use any of the SET options.
Should the LEC QoS configuration be deleted? [No]: yes
Deleted QoS configuration successfully
elan-x LEC QoS Config>
```

ATM Interface QoS Configuration Commands

Table 74. LE Client Quality of Service (QoS) Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
List	Lists the current ATM Interface QoS configuration.
Set	Sets the ATM Interface QoS parameters.
Remove	Removes the QoS configuration of the ATM Interface.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to list the QoS configuration of this ATM Interface. QoS parameters are listed only if at least one parameter has been configured (see following example). Otherwise, no parameters are listed.

Syntax:

list

Example:

```
ATM-I/F 0 QoS> list

          ATM Interface 'Quality of Service' Configuration
          ================================================
                    (ATM interface number = 0  )

     Maximum Reserved Bandwidth for a VCC = 15000 Kbps
     VCC Type ........................... = RESERVED-BANDWIDTH
     Peak Cell Rate ..................... = 20000 Kbps
     Sustained Cell Rate ................ = 5000 Kbps
     QoS Class .......................... = 4
     Maximum Burst Size ................. = 5 frames
ATM-I/F 0 QoS>
```

Set

Use the **set** command to specify ATM Interface QoS parameters.

Syntax:

set max-burst-size
max-reserved-bandwidth
peak-cell-rate
qos-class
sustained-cell-rate
traffic-type

max-burst-size

Sets the desired maximum burst size in frames. See “Maximum Burst Size (max-burst-size)” on page 476 for a more detailed description of this parameter.

Valid Values:

An integer number of frames; must be greater than 0

Default:

1 frame

Example:

```
ATM-I/F 0 QoS Config> se ma
Maximum Burst Size in Kbps [1]? 10000
ATM-I/F 0 QoS Config>
```

max-reserved-bandwidth

Use this option to set the maximum reserved bandwidth allowable for each Data Direct VCC. See “Maximum Reserved Bandwidth (max-reserved-bandwidth)” on page 474 for a more detailed description of this parameter.

Valid Values:

Integer in the range 0 to the line speed of ATM device in Kbps

Default Value:

0

Example:

```
   ATM-I/F 0 QoS> se max-reserved-bandwidth
   Maximum reserved bandwidth acceptable for a data-direct VCC (in Kbps) [0]?
15000
   ATM-I/F 0 QoS>
```

peak-cell-rate

Sets the desired peak cell rate for Data Direct VCCs. See “Peak Cell Rate (peak-cell-rate)” on page 475 for a more detailed description of this parameter.

Valid Values:

An integer value in the range 0 to the line speed of ATM device in Kbps

Default Value:

Line speed of LEC ATM Device in Kbps.

Example:

```
ATM-I/F 0 QoS Config> set peak-cell-rate
Data-Direct VCC Peak Cell Rate in Kbps [1]? 25000
ATM-I/F 0 QoS Config>
```

qos-class

Sets the desired QoS Class for Data Direct VCCs. See “QoS Class (qos-class)” on page 476 for a more detailed description of this parameter.

Valid Values:

0: for Unspecified QoS Class

1: for Specified QoS Class 1

2: for Specified QoS Class 2

3: for Specified QoS Class 3

4: for Specified QoS Class 4

Default Value:

0 (Unspecified QoS Class)

Example:

```
ATM-I/F 0 QoS Config> se qos
Desired QoS Class for Data Direct VCCs [0]? 1
ATM-I/F 0 QoS Config>
```

sustained-cell-rate

Sets the desired sustained cell rate for Data Direct VCCs. See “Sustained Cell Rate (sustained-cell-rate)” on page 475 for a more detailed description of this parameter.

Valid Values:

An integer value in the range 0 to the minimum of max-reserved-bandwidth and peak-cell-rate; specified in Kbps

Default Value

None

Example:

```
ATM-I/F 0 QoS Config> se sus
Data-Direct VCC Sustained Cell Rate in Kbps [1]? 10000
ATM-I/F 0 QoS Config>
```

traffic-type

Sets the desired traffic for Data Direct VCCs. See “Traffic Type (traffic-type)” on page 475 for a more detailed description of this parameter.

Valid Values:

BEST_EFFORT or RESERVED_BANDWIDTH

Default:

BEST EFFORT.

Example:

```
ATM-I/F 0 QoS> set traffic-type
  Choose from:
     (0): Best-Effort
     (1): Reserved Bandwidth
Traffic Type of VCCs [1]? 0
ATM-I/F 0 QoS>
```

Remove

Use the **remove** command to remove the QoS configuration of this ATM Interface.

Syntax:

remove

Example:

```
ATM-I/F 0 QoS> remove
WARNING: This option deletes the QoS configuration.
         To re-configure use any of the SET options.
Should the ATM Interface QoS configuration be deleted? [No]: yes
Deleted QoS SRAM record successfully
ATM-I/F 0 QoS>
```

Accessing the QoS Monitoring Commands

Use the **feature** command from the GWCON process to access the Quality of Service monitoring commands. Enter the **feature** followed by the feature number (6) or short name (QoS). For example:

```
+feature qos
Quality of Service (QoS) - User Monitoring
QoS+
```

Once you access the QoS monitoring prompt, you can select the monitoring of a particular LE Client. To return to the GWCON prompt at any time, enter the exit command at the QoS monitoring prompt.

Alternatively, you can access the QoS Monitoring of an LE Client as follows:

1. At the GWCON prompt (+), enter the network command and the LE Client interface number.
2. At the LE Client monitoring prompt enter **qos-information**.

   Example:

   ```
   +network 3
   ATM Emulated LAN Monitoring
   LEC+qos information
   LE Client QoS Monitoring
   LEC 3 QoS+
   ```

Quality of Service Monitoring Commands

This section summarizes the QoS monitoring commands. Enter these commands at the QoS+ prompt.

Table 75. Quality of Service (QoS) Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
le-client	Gets you to the `LE Client QoS console +` prompt for the selected LE client.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

LE Client QoS Monitoring Commands

This section summarizes the LE Client QoS monitoring commands. Enter the commands from the `LEC num QoS+` prompt.

Table 76. LE Client QoS Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
List	Lists the current LE Client QoS information. Options include: configuration parameters, TLVs, VCCs, and statistics.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to list the QoS related information of this LE Client.

Syntax:

list configuration-parameters

data-direct-VCCs (Detailed Information)

statistics

tlv-information

vcc-information

configuration-parameters

Lists the QoS configuration parameters. Because parameters can be configured for an LE Client, ATM Interface or the ELAN, these parameters are displayed along with a resolved set of parameters that are used by the LE Client.

le-client

The parameters configured for this LE Client which are obtained from the SRAM records. If the SRAM records contain an invalid set of parameters then this column will not display any parameters values.

ATM Interface

The parameters configured for the ATM Interface used by this LE Client. These parameters are obtained from the local SRAM records. If the SRAM records contain an invalid set of parameters then this column will not display any parameter values.

From LECS

The parameters received by this LE Client from the LE Configuration Server. The parameters are received as individual TLVs in the LE_CONFIGURE_RESPONSE control message.

used The resolved set of traffic parameters which are used by for its Data Direct VCCs. If none of the entities is configured with QoS parameters, then the USED parameters represent the default parameters. If parameters are configured for at least one entity, then they are resolved as follows:

- If only the LE Client or the ATM Interface is configured with parameters and either the accept-parms-from-lecs is FALSE or no parameters were received from the LECS, then the configured LE Client or the ATM Interface parameters are used.
- If both the LE Client and the ATM Interface have configured parameters, then the LE Client parameters are used.
- If the accept-parms-from-lecs is TRUE and parameters were received from the LECS, then the LE Client parameters (or the default if the LE Client is not configured) are combined with those received from the LECS to form a complete set of the first six QoS parameters described in "QoS Configuration Parameters" on page 474.
- If the set of the first six QoS parameters described in "QoS Configuration Parameters" on page 474 contains an invalid combination then the parameters from the LECS are rejected. Note that the two flags negotiate-qos and validate-pcr-of-best-effort-vccs are validated independently.

Example:

```
LEC 1 QoS+ list configuration parameters


                ATM LEC Configured QoS  Parameters
                ==================================

      QoS                                        |    LEC      ATM-IF    FROM

   PARAMETER                              USED   |    SRAM     SRAM      LECS

 ------------------------------------------------------------------------------
 Max Reserved Bandwidth (cells/sec) :    23584   |    23584        0     none
                       (Kbits/sec) :    10000   |    10000        0     none
 VCC Type ......................... :   ResvBW   |   ResvBW   BstEft        0
 Peak Cell Rate ........(cells/sec) :    18867   |    18867   365566   365566
                       (Kbits/sec) :     8000   |     8000   155000   155000
 Sustained Cell Rate ...(cells/sec) :    18867   |    18867   365566     none
                       (Kbits/sec) :     8000   |     8000   155000     none
 QoS Class ........................ :        4   |        4        0     none
 Max Burst Size ............(cells) :       95   |       95        0     none
                          (frames) :        1   |        1        0     none
 Validate PCR of Best-Effort VCCs . :       NO   |       NO      n/a     none
 Enable QoS Negotiation ........... :      YES   |      YES      n/a     none
 Accept QoS Parameters from LECS .. :      YES   |      YES      n/a      n/a
 ------------------------------------------------------------------------------
(BstEft = Best Effort, ResvBW = Reserved Bandwidth)
(n/a = not applicable, none = no value is specified)

LEC 1 QoS+
```

data-direct-vccs (Detailed Information)

This option lists the Data Direct VCC information of this LE Client. Similar information is also listed using **list vcc-information**.

Example:

```
LEC 1 QoS+ list data direct vccs

          LEC Data Direct VCCs - QoS Information
          ======================================

Conn Handle = 80, VPI = 0, VCI = 546
        Connection Type = RETRIED CONNECTION PARAMETERS
          TrafficType    = BEST EFFORT VCC
          PCR            = 58962 (25 Mbps)
          SCR            = 58962 (25 Mbps)
          QoS Class      = 0
          Max Burst Size = 0

Conn Handle = 78, VPI = 0, VCI = 544
        Connection Type = PARAMETERS SET BY DESTINATION
          TrafficType    = RESERVED BANDWIDTH VCC
          PCR            = 58962 (25 Mbps)
          SCR            = 16509 (7 Mbps)
```

```
          QoS Class      = 1
          Max Burst Size = 95

LEC 1 QoS+
```

statistics

Counters are maintained for the following statistics:

Successful QoS Connections
Number of RESERVED-BANDWIDTH connections established by the LE Client.

Successful Best-Effort Connections
Number of BEST-EFFORT connections established by the LE Client.

Failed QoS Connections
Number of RESERVED-BANDWIDTH connection requests made by the LE Client that failed.

Failed Best-Effort Connections
Number of BEST-EFFORT connection requests made by the LE Client that failed.

QoS Negotiation Applied
Number of times the QoS negotiation extension was applied. Parameters are negotiated if the LE Client receives the destination LE Client's parameters in an LE_ARP_RESPONSE control message.

PCR Proposal (IBM) Applied
Number of times the IBM Peak Cell Rate Proposal was applied. This proposal recommends using specific rate parameters if signaling at 100 Mbps or 155 Mbps for BEST-EFFORT connections. This allows other participating IBM products (for example, 25-Mbps ATM adapters) to reject a connection based on the signaled peak cell rates.

QoS Connections Accepted
Number of RESERVED-BANDWIDTH connections accepted by this LE Client.

Best-Effort Connections Accepted
Number of BEST-EFFORT connections accepted by this LE Client.

QoS Connections Rejected
Number of RESERVED-BANDWIDTH connection requests received by this LE Client that were rejected.

Best-Effort Connections Rejected
Number of BEST-EFFORT connection requests received by this LE Client that were rejected.

Rejected due to PCR Validation
Number of BEST-EFFORT connections rejected by the LE Client due to validation of Peak Cell Rate when the validate-pcr-of-best-effort-vccs parameter is TRUE.

Example:

```
LEC 1 QoS+ li stat

QoS Statistics: of Data Direct Calls Placed by the LEC
------------------------------------------------------
    Successful QoS Connections          = 0
    Successful Best-Effort Connections  = 1
```

```
    Failed QoS Connections              = 1
    Failed Best-Effort Connections      = 1
    Qos Negotiation Applied             = 0
    PCR Proposal (IBM) Applied          = 0

QoS Statistics: of Data Direct Calls Received by the LEC
--------------------------------------------------------
    QoS Connections Accepted            = 1
    Best-Effort Connections Accepted    = 0
    QoS Connections Rejected            = 0
    Best-Effort Connections Rejected    = 0
    Rejected due to PCR Validation      = 0

LEC 1 QoS+
```

tlv-information

Lists the IBM Traffic Information TLV that this LE Client registered with the LE Server. The TLV is registered only if the LE Client is participating in QoS Negotiation.

Example:

```
LEC 1 QoS+ list tlv

  Traffic Info TLV of the LEC (registered with the LES)
  =====================================================
    TLV Type .........................= 268458498
    TLV Length .......................= 24
    TLV Value:
           Maximum Reserved Bandwidth = 23584 cells/sec (10 Mbps)
           Data Direct VCC Type...... = RESERVED BANDWIDTH VCC
           Data Direct VCC PCR....... = 18867 cells/sec (8 Mbps)
           Data Direct VCC SCR....... = 18867 cells/sec (8 Mbps)
           Data Direct VCC QoS Class  = 4
           Maximum Burst Size         = 95 cells (1 frames)

LEC 1 QoS+
```

vcc-information

Lists all active VCCs of the LE Client. The information includes the traffic parameters of the connections. For BEST-EFFORT connections, the Sustained Cell Rate is displayed to be the same as the Peak Cell Rate, QoS Class and the Maximum Burst Size are displayed as 0.

The Parameter Descriptor entries are:

SrcParms
: Parameters of a connection established by this LE Client.

DestParms
: Parameters of a connection received by this LE Client.

NegoParms
: Parameters of a connection established by the LE Client for which the QoS Negotiation was used.

RetryParms
: Parameters of a connection established by this LE Client after failing at least once.

Example:

```
LEC 1 QoS+ li vcc

                          LEC VCC Table
                          =============

                                                                    Burst
Conn   Conn              Conn          VCC    PCR    SCR   QoS    Size    Parameters
Index  Handle VPI   VCI   Type  Status  Type  (kbps) (kbps) Class (cells) Descriptor
-------------------------------------------------------------------------------------
   2)     69    0   535  Cntrl  Ready  BstEft 155000 155000    0      0   SrcParms
   3)     71    0   537  Cntrl  Ready  BstEft      0      0    0      0   DestParms
   4)     72    0   538  Mcast  Ready  BstEft 155000 155000    0      0   SrcParms
```

```
     5)     74    0   540  Mcast  Ready  BstEft      0      0    0      0   DestParms
     6)     78    0   544  Data   Ready  ResvBW  25000   7000    1     95   DestParms

LEC 1 QoS+
```

Part 3. Appendixes

© Copyright IBM Corp. 1996, 1998

Appendix A. Quick Configuration Reference

Important

If you are attempting to configure or monitor your IBM 8210 and your service terminal is unreadable, see “Service Terminal Display Unreadable” in Mulitprotocol Switched Services (MSS) Server Service and Maintenance Manual.

Quick Configuration Tips

Making Selections

On the panels that you view when using the Quick Configuration program, the information shown in brackets, [ ], is the default. For example:

```
Configure Bridging? (Yes, No, Quit): [Yes]
```

- To use the default `Yes`, press **Enter**.
- To use a value other than the default, such as `No` or `Quit`, choose from the values in the parentheses.
- If no value appears in the brackets, there is no default and you must type a value.

Exiting and Restarting

- To restart the current Quick Configuration section at any time, type **r**. For example, if you are in the Interface Configuration section, type **r** and press **Enter** to return to the beginning of that section.
- To exit Quick Configuration, type **q** and press **Enter**. The `Config>` prompt will appear.
- To restart Quick Configuration from the `Config>` prompt, type **qc** and press **Enter**.

When You’re Done

- Once you have completed your configuration, you must restart the IBM 8210 for the configuration to take effect. At the end of the Quick Configuration program, you are given this option.

Starting the Quick Configuration Program

The following sections describe sample configurations using the Quick Configuration program (**qconfig**).

To start the quick configuration program, enter **qc** at the `Config>` prompt.

The program displays the following panel after starting.

© Copyright IBM Corp. 1996, 1998

```
Router Quick Configuration for the following:

o   Bridging
        Spanning Tree Bridge (STB)
        Source Routing Bridge (SRB)
        Source Routing Transparent Bridge (SRT)
o   Protocols
        IP (including OSPF, RIP, and SNMP)
        IPX

Event Logging will be enabled for all configured subsystems
with logging level 'Standard'

Note: Please be warned that any existing configuration for a particular item
will be removed if that item is configured through Quick Configuration
```

Event logging records system activity, status changes, data transmission and reception, data and internal errors, and service requests. The logging level is set to standard (the default). For more information about error logging, refer to the *Event Logging System Messages Guide*.

During Quick Configuration you can:

1. Configure bridging
2. Configure protocols
3. Restart the router

Configuring LAN Emulation

If you added an ATM device, you will see the following prompts:

```
*********************************************************
LAN Emulation Configuration
*********************************************************

Type 'Yes' to Configure LAN Emulation
Type 'No' to skip LAN Emulation Configuration
Type 'Quit' to exit Quick Config

Configure LAN Emulation? (Yes, No, Quit): [Yes]
```

You can configure either Token-Ring or Ethernet LAN Emulation clients from this question.

Configuring Bridging

```
*********************************************
Bridging Configuration
*********************************************

Type 'Yes' to Configure Bridging
Type 'No' to skip Bridging Configuration
Type 'Quit' to exit Quick Config

Configure Bridging? (Yes, No, Quit): [Yes]
```

1. In response to `Configure Bridging`, take one of the following actions:
   - Enter **y** to display the bridging configuration prompts. The prompts that appear depend on your network configuration.

- Enter **n** to skip the bridging configuration and continue with quick configuration.
- Enter **q** to exit quick configuration. This displays the `Config>` prompt. To reenter quick configuration, enter **qc** after this prompt.

2. If you choose to configure bridging, Spanning Tree Bridging (STB) will be enabled on all LAN interfaces. You will see the following panels:

```
Type 'r' any time at this level to restart Bridging Configuration

STB will be enabled on all LAN interfaces
```

   Enter **y** to configure SRT bridging. Otherwise, enter **n**. For each Token-Ring interface in the configuration, you will be prompted to enable Source Routing on the interface.

```
Configure SRT Bridging? (Yes, No): [Yes]
You are now configuring the Source Routing part of SRT Bridging
Bridge Number (hex) of this Router (1-F): [A]
```

3. Enter a bridge number, which is a hexadecimal value from 1 to F that is unique between two parallel segments.

```
Interface 0 (Port 1) is of type Token Ring
Configure Source Routing on this interface (Yes, No): [Yes]
```

4. Enter **y** to configure source routing on the interface. The console displays the next two lines.

```
Configuring Interface 0 (Port 1)
Segment Number (hex) of this Interface (1-FFF): [A1]
```

   Note: The port number increases by one because source routing bridging does not allow a port number of zero.

   A unique hexadecimal value from 1 to FFF is assigned to each interface. The interfaces on each ring (segment) have the same segment number, but the segment number is unique to each ring.

   These prompts appear for each Token Ring interface.

```
Interface 1 (Port 2) is of type Token Ring
Configure Source Routing on this interface? (Yes, No): [Yes]
Configuring Interface 1 (Port 2)
Segment Number (hex) of this Interface (1-FFF): [A2]
```

   If more than two interfaces are configured for source routing, enter a unique hexadecimal value from 1 to FFF unique for the internal virtual segment.

```
Virtual Segment Number (hex) of this Router (1-FFF): [A4]
```

5. A panel similar to the following is displayed:

```
This is all configured bridging information:

       Interfaces configured for STB:

       Interface #    Port #     Interface Type

           0          1          Token Ring
           1          2          Token Ring

The Source Routing part of SRT Bridging has been enabled

Bridge Number of this Router: A

Interfaces configured for Source Routing:

       Interface #     Port#      Segment #   Interface Type

           0             1          A1        Token Ring
           1             2          A2        Token Ring

Virtual Segment Number of this Router:  A4

Save this Configuration? (Yes, No): [Yes]
```

6. Enter **y** to save the bridging configuration and continue with quick configuration. Enter **n** to re-display the bridging configuration prompts.

   If you enter **y**, the following message appears:

```
Bridging configuration saved
```

Configuring Protocols

After you save the bridging configuration, you will see the following panel:

```
*********************************************
Protocol Configuration
*********************************************

Type 'Yes' to Configure Protocols
Type 'No' to skip Protocol Configuration
Type 'Quit' to exit Quick Config

Configure Protocols? (Yes, No, Quit): [Yes]
```

Take one of the following actions:

- Enter **y** to configure the protocols.
- Enter **n** to skip protocol configuration and continue with quick configuration.
- Enter **q** to exit quick configuration.

You will first configure IP, and then IPX.

Configuring IP

When you answer **y** to the Configure Protocol panel, quick configuration displays the following messages:

```
Type 'r' any time at this level to restart Protocol configuration

Configure IP? (Yes, No): [Yes]
```

1. Take one of the following actions:
   - Enter **y** to configure IP.

- Enter **n** to skip IP configuration and continue with quick configuration.

The following lines appear for each interface.

```
Configuring Per-Interface IP Information

Configuring Interface 0 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [ ] 128.185.141.1
Address Mask: [255.255.0.0]
```

2. Enter the IP address in decimal notation for example, 128.185.142.20. The console displays one of the following error messages if you enter an invalid IP address:

   ```
   Bad address, please try again.

   This address has already been assigned.  Enter a different address
   ```

   Address mask is a decimal value that reflects the IP network or subnetwork to which this interface is attached.

   For more information about IP addressing or address masks, refer to the *Protocol Configuration and Monitoring Reference*, or consult your network administrator.

   ```
   Per-Interface IP Configuration complete

   Configuring IP Routing Information
   Enable Dynamic Routing (Yes, No): [Yes]
   ```

3. Enter **y** if you want the routing protocols (RIP or OSPF) to build the routing tables. Enter **n** to manually add IP address destinations to the routing tables (static routes).

   ```
   Enable OSPF? (Yes, No): [Yes]
   ```

4. Enter **y** to enable the OSPF routing protocol as the primary dynamic IP routing protocol. RIP will be enabled only to send advertisements, not to receive them. Enter **n** if you do not want to use OSPF. RIP will be enabled to send and receive advertisements.

   ```
   OSPF Enabled with Max routes = 1000  and Max routers = 50
   ```

   Max routes is the maximum number of autonomous system (AS) external routes imported into the OSPF routing domain. Max routers is the maximum number of OSPF routers in the routing domain.

```
Routing Configuration Complete

SNMP will be configured with the following parameters:

Community: public
Access:    READONLY

If you plan to use the graphical configuration tool
to download a configuration, it requires the definition
of a community name with read_write_trap access.

Define community with read_write_trap access ? (Yes, No):  [Yes]


This is the information you have entered:

          Interface #        IP Address     Address Mask

             0               128.185.141.1  255.255.255.0
             1               128.185.142.1  255.255.255.0
             2               128.185.143.1  255.255.255.0

OSPF is configured, and RIP is configured only for 'sending'

SNMP has been configured with the following parameters:

     Community: public
     Access:    read_trap

     Community: dana
     Access:    read_write_trap

Save this configuration? (Yes, No): [Yes]
```

5. Enter **y** to save the IP configuration and continue with quick configuration. Enter **n** to re-display the protocol configuration prompts.

Configuring IPX

After you save the IP configuration, you will see the following messages:

```
Configure IPX? (Yes, No): [Yes]
```

1. Enter **y** to configure IPX. Enter **n** to skip IPX configuration and continue with quick configuration.

   You will see messages similar to the following:

   ```
   Type 'r' any time at this level to restart IPX Configuration
   IPX Configuration is already present
   Configure IPX anyway? (Yes, No): [No] yes
   ```

2. Enter **y** to replace the existing configuration. Enter **n** to keep the current configuration and continue.

   ```
   Configuring Per-Interface IPX Information

   Configuring Interface 0 (Token Ring)
   Configure IPX on this interface? (Yes, No): [Yes]
   ```

3. The next messages and your responses depend on whether you are configuring Token-Ring, FDDI, or Ethernet.

   Configuring IPX for Token-Ring:

   a. The following prompt is displayed:

```
Token Ring encapsulation (frame) type? (TOKEN–RING MSB, TOKEN–RING LSB,
    TOKEN–RING_SNAP MSB, TOKEN–RING_SNAP LSB): [TOKEN–RING MSB]
```

b. Enter the encapsulation type used by the IPX protocol on your Token-Ring end stations.

`Token–Ring MSB:`	Most common encapsulation type and the default. The IBM 8210 builds outgoing packets with a 3-byte 802.2 header, (0xE0, 0xE0, 0x03). It sends the source and destination addresses in MSB (most significant bit), or noncanonical, format, which is the native address format for Token-Ring.
`Token–Ring LSB`	Same as Token-Ring MSB except the IBM 8210 sends the addresses in LSB (least significant bit), or canonical, format.
`Token-Ring SNAP MSB`	The IBM 8210 builds outgoing packets with an 8-byte 802.2/SNAP header (0xAA, 0xAA, 0x03, 0x00, 0x00, 0x00, 0x81, 0x37). It sends the source and destination addresses in most significant bit (MSB), or noncanonical, format.
`Token-Ring SNAP LSB`	Same as Token-Ring SNAP MSB except the IBM 8210 sends the addresses in LSB, or canonical, format.

Configuring IPX for Ethernet:

a. The following prompts are displayed:

```
Ethernet encapsulation type? (ETHERNET_8022, ETHERNET_8023, ETHERNET_ii,
ETHERNET_SNAP): [ETHERNET_8023]
```

b. Enter the encapsulation type used by the IPX protocol on your Ethernet end stations.

`Ethernet_8022`	Packet includes an 802.2 header.
`Ethernet_8023`	Uses an IEEE 802.3 packet format without the 802.2 header. This is the default and the default for NetWare versions prior to 4.0. Ethernet 802.3 does not conform to the IEEE 802 standards because it does not include an 802.2 header. It may cause problems with other nodes on the network.
`Ethernet_II`	Uses Ethernet type 8137 as the packet format. This format is required if you are using NetWare VMS on the Ethernet. This is the default for NetWare Versions 4.0 and higher.
`Ethernet_SNAP`	Uses the 802.2 format with a SNAP header. This encapsulation type is meant to be compatible with token-ring SNAP encapsulation. However, it violates IEEE standards and is not interoperable across conformal bridges.

Configuring IPX for FDDI:

a. The following prompts are displayed:

```
FDDI encapsulation (frame) type? (FDDI, FDDI_SNAP): [FDDI_SNAP]
```

b. Enter the encapsulation type used by the IPX Protocol for your FDDI end stations.

`fddi`	Sets the encapsulation type to FDDI IEEE 802.2.
`fddi_snap`	Sets the encapsulation type to FDDI SNAP.

```
Network Number (hex) (1-FFFFFFFD):[1] 1
```

4. Assign an IPX network number to the associated directly connected network. Every IPX interface must have a unique network number.

```
Configuring Interface 1 (WAN PPP)
Configure IPX on this interface? (Yes, No): [Yes]
Network Number (hex) (1-FFFFFFFD): [1] 2

Enable IPXWAN? (Yes, No): [No] yes

Configuring Interface 2 (WAN PPP)
Configure IPX on this interface? (Yes, No): [Yes]
Network Number (hex) (1-FFFFFFFD):[1] 3

Enable IPXWAN? (Yes, No): [No] yes

Host Number for Serial Lines: (000000000000) 1

Configure IPXWAN NodeID? (Yes, No): [Yes]
NodeID (hex) (1 - FFFFFFFD): [1] 4
```

   If enabled, the IPXWAN protocol negotiates routing parameters to be used on the PPP serial interface before IPX packet forwarding begins. IPXWAN is not required to forward IPX packets on PPP serial interfaces. The IPXWAN Node ID is a unique IPX network number that identifies the router, and is required if IPXWAN is enabled on any network interfaces.

5. Host number is a unique 12-digit hexadecimal value assigned to an IPX router. It is required because serial lines do not have hardware node addresses from which to build a host number.

```
This is the information you have entered:

               Per-Interface Configuration Information

Cir   Ifc   IPX Net(hex)   Encapsulation       IPXWAN

1     1     10            ETHERNET_8023       Not Configured
2     3     300                               Not Configured
3     5     400                               Not Configured
4     6     600                               Enabled


  Host Number for Serial Lines: 0002210A0000
  IPXWAN Node ID = 2210A
  IPX Router Name = ipxwan_router-2210A


Save this configuration? (Yes, No): [Yes]
```

6. Enter **y** to save the IPX configuration and continue with quick configuration. Enter **n** to re-display the IPX configuration prompts.

   If you enter **y**, the following message appears:

```
IPX configuration saved
```

Restarting the IBM 8210

After configuring the protocols, you will receive the following message:

```
Quick Config Done
Do you want to write this configuration? (Yes, No): [Yes]
```

Enter **y** to save your changes and display the following information:

```
Default config file written successfully.

Configuration was written.
The system must be restarted for this configuration to take effect.
```

Enter **reload** at the OPCON prompt (*) to restart the IBM 8210 with the new configuration. To change or view the current configuration, enter **qc**.

Appendix B. Abbreviations

AAL ATM Adaptation Layer

AAL-5 ATM Adaptation Layer 5

AARP AppleTalk Address Resolution Protocol

ABR area border router

ack acknowledgment

AIX Advanced Interactive Executive

AMA arbitrary MAC addressing

AMP active monitor present

ANSI American National Standards Institute

AP2 AppleTalk Phase 2

APPN Advanced Peer-to-Peer Networking

ARE all-routes explorer

ARI ATM real interface

ARI/FCI
address recognized indicator/frame copied indicator

ARP Address Resolution Protocol

AS autonomous system

ASBR autonomous system boundary router

ASCII American National Standard Code for Information Interchange

ASN.1 abstract syntax notation 1

ASRT adaptive source routing transparent

ASYNC
asynchronous

ATCP AppleTalk Control Protocol

ATM Asynchronous Transfer Mode

ATMARP
ARP in Classical IP

ATP AppleTalk Transaction Protocol

AUI attachment unit interface

AVI ATM virtual interface

ayt are you there

BAN Boundary Access Node

BBCM Bridging Broadcast Manager

BCM BroadCast Manager

BECN backward explicit congestion notification

BGP Border Gateway Protocol

BGP Border Growth Protocol

© Copyright IBM Corp. 1996, 1998

BNC bayonet Niell-Concelman

BNCP Bridging Network Control Protocol

BOOTP
BOOT protocol

BPDU bridge protocol data unit

bps bits per second

bandwidth reservation

BSD Berkeley software distribution

BTP BOOTP relay agent

BTU basic transmission unit

BUS Broadcast and Unknown Server

CAM content-addressable memory

CCITT Consultative Committee on International Telegraph and Telephone

CD collision detection

CGWCON
Gateway Console

CIDR Classless Inter-Domain Routing

CIP Classical IP

CIPC Classical IP Client

CIR committed information rate

CLNP Connectionless-Mode Network Protocol

CPU central processing unit

CRC cyclic redundancy check

CRS configuration report server

CTS clear to send

CUD call user data

DAF destination address filtering

DB database

DBsum
database summary

DCD data channel received line signal detector

DCE data circuit-terminating equipment

DCS directly connected server

DDLC dual data-link controller

DDN Defense Data Network

DDP Datagram Delivery Protocol

DDT Dynamic Debugging Tool

DHCP Dynamic Host Configuration Protocol

dir directly connected

DL data link

DLC data link control

DLCI data link connection identifier

DLS data link switching

DLSw data link switching

DMA direct memory access

DNA Digital Network Architecture

DNCP DECnet Protocol Control Protocol

DNIC Data Network Identifier Code

DoD Department of Defense

DOS Disk Operating System

DR designated router

DRAM Dynamic Random Access Memory

DSAP destination service access point

DSE data switching equipment

DSE data switching exchange

DSR data set ready

DSU data service unit

DTE data terminal equipment

DTR data terminal ready

Dtype destination type

DVMRP
Distance Vector Multicast Routing Protocol

E1 2.048 Mbps transmission rate

EDEL end delimiter

EDI error detected indicator

EGP Exterior Gateway Protocol

EIA Electronics Industries Association

ELAN Emulated Local Area Network

ELAP EtherTalk Link Access Protocol

ELS Event Logging System

ESI End System Identifier

EST Eastern Standard Time

Eth Ethernet

fa-ga functional address-group address

FCS frame check sequence

FECN forward explicit congestion notification

FIFO first in, first out

FLT filter library

FR Frame Relay

FRL Frame Relay

FTP File Transfer Protocol

GMT Greenwich Mean Time

GOSIP
Government Open Systems Interconnection Profile

GTE General Telephone Company

GWCON
Gateway Console

HDLC high-level data link control

HEX hexadecimal

HST TCP/IP host services

HTF host table format

IBD Integrated Boot Device

ICMP Internet Control Message Protocol

ICP Internet Control Protocol

ID identification

IDP Initial Domain Part

IDP Internet Datagram Protocol

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

Ifc# interface number

IGP interior gateway protocol

ILMI Interim Local Management Interface

InARP Inverse Address Resolution Protocol

IP Internet Protocol

IPCP IP Control Protocol

IPPN IP Protocol Network

IPX Internetwork Packet Exchange

IPXCP IPX Control Protocol

ISDN integrated services digital network

ISO International Organization for Standardization

Kbps kilobits per second

LAN local area network

LAPB link access protocol-balanced

LAT local area transport

LCP Link Control Protocol

LE LAN Emulation

LEC LAN Emulation Client

LED light-emitting diode

LECS LAN Emulation Configuration Server

LES LAN Emulation Server

LES-BUS
LAN Emulation Server - Broadcast and Unknown Server

LF largest frame; line feed

LIS Logical IP subnet

LLC logical link control

LLC2 logical link control 2

LMI local management interface

LRM LAN reporting mechanism

LS link state

LSA link state advertisement

LSB least significant bit

LSI LANE Shortcuts Interface

LSreq link state request

LSrxl link state retransmission list

LU logical unit

MAC medium access control

Mb megabit

MB megabyte

Mbps megabits per second

MBps megabytes per second

MC multicast

MCF MAC filtering

MIB Management Information Base

MIB II Management Information Base II

MILNET
military network

MOS Micro Operating System

MOSDDT
Micro Operating System Dynamic Debugging Tool

MOSPF
Open Shortest Path First with multicast extensions

MSB most significant bit

MSDU MAC service data unit

MSS Multiprotocol Switched Services

MTU maximum transmission unit

nak not acknowledged

NBMA Non-Broadcast Multiple Access

NBP Name Binding Protocol

NBR neighbor

NCP Network Control Protocol

NCP Network Core Protocol

NetBIOS
Network Basic Input/Output System

NHRP Next Hop Resolution Protocol

NIST National Institute of Standards and Technology

NPDU Network Protocol Data Unit

NRZ non-return-to-zero

NRZI non-return-to-zero inverted

NSAP Network Service Access Point

NSF National Science Foundation

NSFNET
National Science Foundation NETwork

NVCNFG
nonvolatile configuration

OPCON
Operator Console

OSI open systems interconnection

OSICP
OSI Control Protocol

OSPF Open Shortest Path First

OUI organization unique identifier

PC personal computer

PCR peak cell rate

PDN public data network

PING Packet internet groper

PDU protocol data unit

PID process identification

P-P Point-to-Point

PPP Point-to-Point Protocol

PROM programmable read-only memory

PU physical unit

PVC permanent virtual circuit

QoS Quality of Service

RAM random access memory

RD route descriptor

REM ring error monitor

REV receive

RFC Request for Comments

RI ring indicator; routing information

RIF routing information field

RII routing information indicator

RIP Routing Information Protocol

RISC reduced instruction-set computer

RNR receive not ready

ROM read-only memory

ROpcon
Remote Operator Console

RPS ring parameter server

RTMP Routing Table Maintenance Protocol

RTP RouTing update Protocol

RTS request to send

Rtype route type

rxmits retransmissions

rxmt retransmit

SAF source address filtering

SAP service access point

SAP Service Advertising Protocol

SCR sustained cell rate

SCSP Server Cache Synchronization Protocol

sdel start delimiter

SDLC SDLC relay, synchronous data link control

SDU Service Data Unit

SGID server group id

seqno sequence number

SGMP Simple Gateway Monitoring Protocol

SL serial line

SLIP Serial Line IP

SMP standby monitor present

SMTP Simple Mail Transfer Protocol

SNA Systems Network Architecture

SNAP Subnetwork Access Protocol
SubNetwork Attachment Point

SNMP Simple Network Management Protocol

SNPA subnetwork point of attachment

SPF OSPF intra-area route

SPE1 OSPF external route type 1

SPE2 OSPF external route type 2

SPIA OSPF inter-area route type

SPID service profile ID

SPX Sequenced Packet Exchange

SQE signal quality error

SRAM static random access memory

SRB source routing bridge

SRF specifically routed frame

SRLY SDLC relay

SRT source routing transparent

SR-TB
source routing-transparent bridge

STA static

STB spanning tree bridge

STE spanning tree explorer

STP shielded twisted pair; spanning tree protocol

SVC switched virtual circuit

SVN Switched Virtual Networking

TB transparent bridge

TCN topology change notification

TCP Transmission Control Protocol

TCP/IP
Transmission Control Protocol/Internet Protocol

TEI terminal point identifier

TFTP Trivial File Transfer Protocol

TKR token ring

TLV Type/Length/Value

TMO timeout

TOS type of service

TSF transparent spanning frames

TTL time to live

TTY teletypewriter

TX transmit

UA unnumbered acknowledgment

UDP User Datagram Protocol

UI unnumbered information

UNI User-Network Interface

UTP unshielded twisted pair

VCC Virtual Channel connection

VINES VIrtual NEtworking System

VIR variable information rate

VL virtual link

VNI Virtual Network Interface

VR virtual route

WAN wide area network

WRS WAN restoral

X.25 packet-switched networks

X.251 X.25 physical layer

X.252 X.25 frame layer

X.253 X.25 packet layer

XID exchange identification

XNS Xerox Network Systems

XSUM checksum

ZIP AppleTalk Zone Information Protocol

ZIP2 AppleTalk Zone Information Protocol 2

ZIT Zone Information Table

Glossary

This glossary includes terms and definitions from:

- The *American National Standard Dictionary for Information Systems* , ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by the symbol (A) after the definition.
- The ANSI/EIA Standard—440-A, *Fiber Optic Terminology* Copies may be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Definitions are identified by the symbol (E) after the definition.
- The *Information Technology Vocabulary* developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- The *IBM Dictionary of Computing* , New York: McGraw-Hill, 1994.
- Internet Request for Comments: 1208, *Glossary of Networking Terms*
- Internet Request for Comments: 1392, *Internet Users' Glossary*
- The *Object-Oriented Interface Design: IBM Common User Access Guidelines* , Carmel, Indiana: Que, 1992.

The following cross-references are used in this glossary:

Contrast with:
This refers to a term that has an opposed or substantively different meaning.

Synonym for:
This indicates that the term has the same meaning as a preferred term, which is defined in its proper place in the glossary.

Synonymous with:
This is a backward reference from a defined term to all other terms that have the same meaning.

See: This refers the reader to multiple-word terms that have the same last word.

See also:
This refers the reader to terms that have a related, but not synonymous, meaning.

A

AAL. ATM Adaptation Layer, the layer that adapts user data to/from the ATM network by adding/removing headers and segmenting/reassembling the data into/from cells.

AAL-5. ATM Adaptation Layer 5, one of several standard AALs. AAL-5 was designed for data communications, and is used by LAN Emulation and Classical IP.

abstract syntax. A data specification that includes all distinctions that are needed in data transmissions, but that omits (abstracts) other details such as those that depend on specific computer architectures. See also *abstract syntax notation 1 (ASN.1)* and *basic encoding rules (BER)*.

abstract syntax notation 1 (ASN.1). The Open Systems Interconnection (OSI) method for abstract syntax specified in the following standards:

- ITU-T Recommendation X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T Recommendation X.680 (1994) | ISO/IEC 8824-1: 1994

See also *basic encoding rules (BER)*.

ACCESS. In the Simple Network Management Protocol (SNMP), the clause in a Management Information Base (MIB) module that defines the minimum level of support that a managed node provides for an object.

acknowledgment. (1) The transmission, by a receiver, of acknowledge characters as an affirmative response to a sender. (T) (2) An indication that an item sent was received.

active monitor. In a token-ring network, a function performed at any one time by one ring station that initiates the transmission of tokens and provides token error recovery facilities. Any active adapter on the ring has the ability to provide the active monitor function if the current active monitor fails.

© Copyright IBM Corp. 1996, 1998

address. In data communication, the unique code assigned to each device, workstation, or user connected to a network.

address mapping table (AMT). A table, maintained within the AppleTalk router, that provides a current mapping of node addresses to hardware addresses.

address mask. For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address. Synonymous with *subnet mask* and *subnetwork mask*.

address resolution. (1) A method for mapping network-layer addresses to media-specific addresses. (2) See also *Address Resolution Protocol (ARP)* and *AppleTalk Address Resolution Protocol (AARP)*.

Address Resolution Protocol (ARP). (1) In the Internet suite of protocols, the protocol that dynamically maps an IP address to an address used by a supporting metropolitan or local area network such as Ethernet or token-ring. (2) See also *Reverse Address Resolution Protocol (RARP)*.

addressing. In data communication, the way in which a station selects the station to which it is to send data.

adjacent nodes. Two nodes connected together by at least one path that connects no other node. (T)

Administrative Domain. A collection of hosts and routers, and the interconnecting networks, managed by a single administrative authority.

Advanced Peer-to-Peer Networking (APPN). An extension to SNA featuring (a) greater distributed network control that avoids critical hierarchical dependencies, thereby isolating the effects of single points of failure; (b) dynamic exchange of network topology information to foster ease of connection, reconfiguration, and adaptive route selection; (c) dynamic definition of network resources; and (d) automated resource registration and directory lookup. APPN extends the LU 6.2 peer orientation for end-user services to network control and supports multiple LU types, including LU 2, LU 3, and LU 6.2.

Advanced Peer-to-Peer Networking (APPN) end node. A node that provides a broad range of end-user services and supports sessions between its local control point (CP) and the CP in an adjacent network node. It uses these sessions to dynamically register its resources with the adjacent CP (its network node server), to send and receive directory search requests, and to obtain management services. An APPN end node can also attach to a subarea network as a peripheral node or to other end nodes.

Advanced Peer-to-Peer Networking (APPN) network. A collection of interconnected network nodes and their client end nodes.

Advanced Peer-to-Peer Networking (APPN) network node. A node that offers a broad range of end-user services and that can provide the following:

- Distributed directory services, including registration of its domain resources to a central directory server
- Topology database exchanges with other APPN network nodes, enabling network nodes throughout the network to select optimal routes for LU-LU sessions based on requested classes of service
- Session services for its local LUs and client end nodes
- Intermediate routing services within an APPN network

Advanced Peer-to-Peer Networking (APPN) node. An APPN network node or an APPN end node.

alert. A message sent to a management services focal point in a network to identify a problem or an impending problem.

all-stations address. In communications, synonym for *broadcast address*.

American National Standards Institute (ANSI). An organization consisting of producers, consumers, and general interest groups, that establishes the procedures by which accredited organizations create and maintain voluntary industry standards in the United States. (A)

analog. (1) Pertaining to data consisting of continuously variable physical quantities. (A) (2) Contrast with *digital*.

AppleTalk. A network protocol developed by Apple Computer, Inc. This protocol is used to interconnect network devices, which can be a mixture of Apple and non-Apple products.

AppleTalk Address Resolution Protocol (AARP). In AppleTalk networks, a protocol that (a) translates AppleTalk node addresses into hardware addresses and (b) reconciles addressing discrepancies in networks that support more than one set of protocols.

AppleTalk Transaction Protocol (ATP). In AppleTalk networks, a protocol that provides client/server request and response functions for hosts accessing the Zone Information Protocol (ZIP) for zone information.

APPN network. See *Advanced Peer-to-Peer Networking (APPN) network*.

APPN network node. See *Advanced Peer-to-Peer Networking (APPN) network node*.

arbitrary MAC addressing (AMA). In DECnet architecture, an addressing scheme used by DECnet Phase IV-Prime that supports universally administered addresses and locally administered addresses.

area. In Internet and DECnet routing protocols, a subset of a network or gateway grouped together by

definition of the network administrator. Each area is self-contained; knowledge of an area's topology remains hidden from other areas.

asynchronous (ASYNC). Pertaining to two or more processes that do not depend upon the occurrence of specific events such as common timing signals. (T)

ATM. Asynchonous Transfer Mode, a connection-oriented, high-speed networking technology based on cell switching.

ATMARP. ARP in Classical IP.

attachment unit interface (AUI). In a local area network, the interface between the medium attachment unit and the data terminal equipment within a data station. (I) (A)

authentication failure. In the Simple Network Management Protocol (SNMP), a trap that may be generated by an authentication entity when a requesting client is not a member of the SNMP community.

autonomous system. In TCP/IP, a group of networks and routers under one administrative authority. These networks and routers cooperate closely to propagate network reachability (and routing) information among themselves using an interior gateway protocol of their choice.

autonomous system number. In TCP/IP, a number assigned to an autonomous system by the same central authority that also assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

BCM. BroadCast Manager, an IBM extension to LAN Emulation designed to limit the effects of broadcast frames.

backbone. (1) In a local area network multiple-bridge ring configuration, a high-speed link to which the rings are connected by means of bridges or routers. A backbone may be configured as a bus or as a ring. (2) In a wide area network, a high-speed link to which nodes or data switching exchanges (DSEs) are connected.

backbone network. A central network to which smaller networks, normally of lower speed, connect. The backbone network usually has a much higher capacity than the networks it helps interconnect or is a wide-area network (WAN) such as a public packet-switched datagram network.

backbone router. (1) A router used to transmit data between areas. (2) One in a series of routers that is used to interconnect networks into a larger internet.

Bandwidth. The bandwidth of an optical link designates the information-carrying capacity of the link and is related to the maximum bit rate that a fiber link can support.

basic transmission unit (BTU). In SNA, the unit of data and control information passed between path control components. A BTU can consist of one or more path information units (PIUs).

bootstrap. (1) A sequence of instructions whose execution causes additional instructions to be loaded and executed until the complete computer program is in storage. (T) (2) A technique or device designed to bring itself into a desired state by means of its own action, for example, a machine routine whose first few instructions are sufficient to bring the rest of itself into the computer from an input device. (A)

baud. In asynchronous transmission, the unit of modulation rate corresponding to one unit interval per second; that is, if the duration of the unit interval is 20 milliseconds, the modulation rate is 50 baud. (A)

Border Gateway Protocol (BGP). An Internet Protocol (IP) routing protocol used between domains and autonomous systems. Contrast with *Exterior Gateway Protocol (EGP)*.

border router. In Internet communications, a router, positioned at the edge of an autonomous system, that communicates with a router that is positioned at the edge of a different autonomous system.

bridge. A functional unit that interconnects multiple LANs (locally or remotely) that use the same logical link control protocol but that can use different medium access control protocols. A bridge forwards a frame to another bridge based on the medium access control (MAC) address.

bridge identifier. An 8-byte field, used in a spanning tree protocol, composed of the MAC address of the port with the lowest port identifier and a user-defined value.

bridging. In LANs, the forwarding of a frame from one LAN segment to another. The destination is specified by the medium access control (MAC) sublayer address encoded in the destination address field of the frame header.

broadcast. (1) Transmission of the same data to all destinations. (T) (2) Simultaneous transmission of data to more than one destination. (3) Contrast with *multicast*.

broadcast address. In communications, a station address (eight 1's) reserved as an address common to all stations on a link. Synonymous with *all-stations address*.

BUS. Broadcast and Unknown Server, a LAN Emulation Service component responsible for the delivery of multicast and unknown unicast frames.

C

cache. (1) A special-purpose buffer storage, smaller and faster than main storage, used to hold a copy of instructions and data obtained from main storage and likely to be needed next by the processor. (T) (2) A buffer storage that contains frequently accessed instructions and data; it is used to reduce access time. (3) An optional part of the directory database in network nodes where frequently used directory information may be stored to speed directory searches. (4) To place, hide, or store in a cache.

call request packet. (1) A call supervision packet that a data terminal equipment (DTE) transmits to ask that a connection for a call be established throughout the network. (2) In X.25 communications, a call supervision packet transmitted by a DTE to ask for a call establishment through the network.

canonical address. In LANs, the IEEE 802.1 format for the transmission of medium access control (MAC) addresses for token-ring and Ethernet adapters. In canonical format, the least significant (rightmost) bit of each address byte is transmitted first. Contrast with *noncanonical address*.

carrier. An electric or electromagnetic wave or pulse train that may be varied by a signal bearing information to be transmitted over a communication system. (T)

carrier detect. Synonym for *received line signal detector (RLSD)*.

carrier sense. In a local area network, an ongoing activity of a data station to detect whether another station is transmitting. (T)

carrier sense multiple access with collision detection (CSMA/CD). A protocol that requires carrier sense and in which a transmitting data station that detects another signal while transmitting, stops sending, sends a jam signal, and then waits for a variable time before trying again. (T) (A)

channel. (1) A path along which signals can be sent, for example, data channel, output channel. (A) (2) A functional unit, controlled by the processor, that handles the transfer of data between processor storage and local peripheral equipment.

channel service unit (CSU). A unit that provides the interface to a digital network. The CSU provides line conditioning (or equalization) functions, which keep the signal's performance consistent across the channel bandwidth; signal reshaping, which constitutes the binary pulse stream; and loopback testing, which includes the transmission of test signals between the CSU and the network carrier's office channel unit. See also *data service unit (DSU)*.

checksum. (1) The sum of a group of data associated with the group and used for checking purposes. (T) (2) In error detection, a function of all bits in a block. If the written and calculated sums do not agree, an error is indicated. (3) On a diskette, data written in a sector for error detection purposes; a calculated checksum that does not match the checksum of data written in the sector indicates a bad sector. The data are either numeric or other character strings regarded as numeric for the purpose of calculating the checksum.

CIP. Classical IP.

CIPC. Classical IP Client.

Classical IP. An IETF standard for ATM-attached hosts to communicate using IP over ATM.

Classical IP Client. A Classical IP component that represents users of the Logical IP Subnet.

circuit switching. (1) A process that, on demand, connects two or more data terminal equipment (DTEs) and permits the exclusive use of a data circuit between them until the connection is released. (I) (A) (2) Synonymous with *line switching*.

class A network. In Internet communications, a network in which the high-order (most significant) bit of the IP address is set to 0 and the host ID occupies the three low-order octets.

class B network. In Internet communications, a network in which the two high-order (most significant and next-to-most significant) bits of the IP address are set to 1 and 0, respectively, and the host ID occupies the two low-order octets.

class of service (COS). A set of characteristics (such as route security, transmission priority, and bandwidth) used to construct a route between session partners. The class of service is derived from a mode name specified by the initiator of a session.

client. (1) A functional unit that receives shared services from a server. (T) (2) A user.

client/server. In communications, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.

clocking. (1) In binary synchronous communication, the use of clock pulses to control synchronization of data and control characters. (2) A method of controlling the number of data bits sent on a telecommunication line in a given time.

collision. An unwanted condition that results from concurrent transmissions on a channel. (T)

collision detection. In carrier sense multiple access with collision detection (CSMA/CD), a signal indicating that two or more stations are transmitting simultaneously.

Committed information rate. The maximum amount of data in bits that the network agrees to deliver.

community. In the Simple Network Management Protocol (SNMP), an administrative relationship between entities.

community name. In the Simple Network Management Protocol (SNMP), a string of octets identifying a community.

compression. (1) The process of eliminating gaps, empty fields, redundancies, and unnecessary data to shorten the length of records or blocks. (2) Any encoding to reduce the number of bits used to represent a given message or record.

configuration. (1) The manner in which the hardware and software of an information processing system are organized and interconnected. (T) (2) The devices and programs that make up a system, subsystem, or network.

configuration file. A file that specifies the characteristics of a system device or network.

configuration parameter. A variable in a configuration definition, the values of which can characterize the relationship of a product to other products in the same network or can define characteristics of the product itself.

configuration report server (CRS). In the IBM Token-Ring Network Bridge Program, the server that accepts commands from the LAN Network Manager (LNM) to get station information, set station parameters, and remove stations on its ring. This server also collects and forwards configuration reports generated by stations on its ring. The configuration reports include the new active monitor reports and the nearest active upstream neighbor (NAUN) reports.

congestion. See *network congestion*.

control point (CP). (1) A component of an APPN or LEN node that manages the resources of that node. In an APPN node, the CP is capable of engaging in CP-CP sessions with other APPN nodes. In an APPN network node, the CP also provides services to adjacent end nodes in the APPN network. (2) A component of a node that manages resources of that node and optionally provides services to other nodes in the network. Examples are a system services control point (SSCP) in a type 5 subarea node, a network node control point (NNCP) in an APPN network node, and an end node control point (ENCP) in an APPN or LEN end node. An SSCP and an NNCP can provide services to other nodes.

control point management services (CPMS). A component of a control point, consisting of management services function sets, that provides facilities to assist in performing problem management, performance and accounting management, change management, and configuration management. Capabilities provided by the CPMS include sending requests to physical unit management services (PUMS) to test system resources, collecting statistical information (for example, error and performance data) from PUMS about the system resources, and analyzing and presenting test results and statistical information collected about the system resources. Analysis and presentation responsibilities for problem determination and performance monitoring can be distributed among multiple CPMSs.

control point management services unit (CP-MSU). The message unit that contains management services data and flows between management services function sets. This message unit is in general data stream (GDS) format. See also *management services unit (MSU)* and *network management vector transport (NMVT)*.

D

D-bit. Delivery-confirmation bit. In X.25 communications, the bit in a data packet or call-request packet that is set to 1 if end-to-end acknowledgment (delivery confirmation) is required from the recipient.

daemon. A program that runs unattended to perform a standard service. Some daemons are triggered automatically to perform their task; others operate periodically.

data carrier detect (DCD). Synonym for *received line signal detector (RLSD)*.

data circuit. (1) A pair of associated transmit and receive channels that provide a means of two-way data communication. (I) (2) In SNA, synonym for *link connection*. (3) See also *physical circuit* and *virtual circuit*.

Notes:

1. Between data switching exchanges, the data circuit may include data circuit-terminating equipment (DCE), depending on the type of interface used at the data switching exchange.
2. Between a data station and a data switching exchange or data concentrator, the data circuit includes the data circuit-terminating equipment at the data station end, and may include equipment similar to a DCE at the data switching exchange or data concentrator location.

data circuit-terminating equipment (DCE). In a data station, the equipment that provides the signal

conversion and coding between the data terminal equipment (DTE) and the line. (I)

Notes:

1. The DCE may be separate equipment or an integral part of the DTE or of the intermediate equipment.
2. A DCE may perform other functions that are usually performed at the network end of the line.

data link connection identifier (DLCI). The numeric identifier of a frame-relay subport or PVC segment in a frame-relay network. Each subport in a single frame-relay port has a unique DLCI. The following table, excerpted from the American National Standards Institute (ANSI) Standard T1.618 and the International Telegraph and Telephone Consultative Committee (ITU-T/CCITT) Standard Q.922, indicates the functions associated with certain DLCI values:

DLCI Values	Function
0	in-channel signaling
1–15	reserved
16–991	assigned using frame-relay connection procedures
992–1007	layer 2 management of frame-relay bearer service
1008–1022	reserved
1023	in-channel layer management

data link control (DLC). A set of rules used by nodes on a data link (such as an SDLC link or a token ring) to accomplish an orderly exchange of information.

data link control (DLC) layer. In SNA, the layer that consists of the link stations that schedule data transfer over a link between two nodes and perform error control for the link. Examples of data link control are SDLC for serial-by-bit link connection and data link control for the System/370 channel.

Note: The DLC layer is usually independent of the physical transport mechanism and ensures the integrity of data that reaches the higher layers.

data link layer. In the Open Systems Interconnection reference model, the layer that provides services to transfer data between entities in the network layer over a communication link. The data link layer detects and possibly corrects errors that may occur in the physical layer. (T)

data link level. (1) In the hierarchical structure of a data station, the conceptual level of control or processing logic between high level logic and the data link that maintains control of the data link. The data link level performs such functions as inserting transmit bits and deleting receive bits; interpreting address and control fields; generating, transmitting, and interpreting commands and responses; and computing and interpreting frame check sequences. See also *packet level* and *physical level*. (2) In X.25 communications, synonym for *frame level*.

data link switching (DLSw). A method of transporting network protocols that use IEEE 802.2 logical link control (LLC) type 2. SNA and NetBIOS are examples of protocols that use LLC type 2. See also *encapsulation* and *spoofing*.

data packet. In X.25 communications, a packet used for the transmission of user data on a virtual circuit at the DTE/DCE interface.

data service unit (DSU). A device that provides a digital data service interface directly to the data terminal equipment. The DSU provides loop equalization, remote and local testing capabilities, and a standard EIA/CCITT interface.

data set ready (DSR). Synonym for *DCE ready*.

data switching exchange (DSE). The equipment installed at a single location to provide switching functions, such as circuit switching, message switching, and packet switching. (I)

data terminal equipment (DTE). That part of a data station that serves as a data source, data sink, or both. (I) (A)

data terminal ready (DTR). A signal to the modem used with the EIA 232 protocol.

data transfer rate. The average number of bits, characters, or blocks per unit time passing between corresponding equipment in a data transmission system. (I)

Notes:

1. The rate is expressed in bits, characters, or blocks per second, minute, or hour.
2. Corresponding equipment should be indicated; for example, modems, intermediate equipment, or source and sink.

datagram. (1) In packet switching, a self-contained packet, independent of other packets, that carries information sufficient for routing from the originating data terminal equipment (DTE) to the destination DTE without relying on earlier exchanges between the DTEs and the network. (I) (2) In TCP/IP, the basic unit of information passed across the Internet environment. A datagram contains a source and destination address along with the data. An Internet Protocol (IP) datagram consists of an IP header followed by the transport layer data. (3) See also *packet* and *segment*.

Datagram Delivery Protocol (DDP). In AppleTalk networks, a protocol that provides network connectivity by means of connectionless socket-to-socket delivery service on the internet layer.

DCE ready. In the EIA 232 standard, a signal that indicates to the data terminal equipment (DTE) that the local data circuit-terminating equipment (DCE) is connected to the communication channel and is ready to send data. Synonymous with *data set ready (DSR)*.

DECnet. A network architecture that defines the operation of a family of software modules, databases, and hardware components typically used to tie Digital Equipment Corporation systems together for resource sharing, distributed computation, or remote system configuration. DECnet network implementations follow the Digital Network Architecture (DNA) model.

default. Pertaining to an attribute, condition, value, or option that is assumed when none is explicitly specified. (I)

designated router. A router that informs end nodes of the existence and identity of other routers. The selection of the designated router is based upon the router with the highest priority. When several routers share the highest priority, the router with the highest station address is selected.

destination node. The node to which a request or data is sent.

destination port. The 8-port asynchronous adapter that serves as a connection point with a serial service.

destination service access point (DSAP). In SNA and TCP/IP, a logical address that allows a system to route data from a remote device to the appropriate communications support. Contrast with *source service access point (SSAP)*.

device. A mechanical, electrical, or electronic contrivance with a specific purpose.

digital. (1) Pertaining to data that consist of digits. (T) (2) Pertaining to data in the form of digits. (A) (3) Contrast with *analog*.

Digital Network Architecture (DNA). The model for all DECnet hardware and software implementations.

direct memory access (DMA). The system facility that allows a device on the Micro Channel bus to get direct access to the system or bus memory without the intervention of the system processor.

directory. A table of identifiers and references to the corresponding items of data. (I) (A)

directory service (DS). An application service element that translates the symbolic names used by application processes into the complete network addresses used in an OSI environment. (T)

directory services (DS). A control point component of an APPN node that maintains knowledge of the location of network resources.

disable. To make nonfunctional.

disabled. (1) Pertaining to a state of a processing unit that prevents the occurrence of certain types of interruptions. (2) Pertaining to the state in which a transmission control unit or audio response unit cannot accept incoming calls on a line.

domain. (1) That part of a computer network in which the data processing resources are under common control. (T) (2) In Open Systems Interconnection (OSI), a part of a distributed system or a set of managed objects to which a common policy applies. (3) See *Administrative Domain* and *domain name*.

domain name. In the Internet suite of protocols, a name of a host system. A domain name consists of a sequence of subnames separated by a delimiter character. For example, if the fully qualified domain name (FQDN) of a host system is `ralvm7.vnet.ibm.com`, each of the following is a domain name:

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

domain name server. In the Internet suite of protocols, a server program that supplies name-to-address translation by mapping domain names to IP addresses. Synonymous with *name server*.

Domain Name System (DNS). In the Internet suite of protocols, the distributed database system used to map domain names to IP addresses.

dotted decimal notation. The syntactical representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 with periods (dots) separating them. It is used to represent IP addresses.

dump. (1) Data that has been dumped. (T) (2) To copy the contents of all or part of virtual storage for the purpose of collecting error information.

dynamic reconfiguration (DR). The process of changing the network configuration (peripheral PUs and LUs) without regenerating complete configuration tables or deactivating the affected major node.

Dynamic Routing. Routing using learned routes rather than routes statically configured at initialization.

E

echo. In data communication, a reflected signal on a communications channel. For example, on a communications terminal, each signal is displayed twice, once when entered at the local terminal and again when returned over the communications link. This allows the signals to be checked for accuracy.

EIA 232. In data communication, a specification of the Electronic Industries Association (EIA) that defines the

interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE), using serial binary data interchange.

ELAN. Emulated Local Area Network, a LAN segment implemented with ATM technology.

Electronic Industries Association (EIA). An organization of electronics manufacturers that advances the technological growth of the industry, represents the views of its members, and develops industry standards.

encapsulation. (1) In communications, a technique used by layered protocols by which a layer adds control information to the protocol data unit (PDU) from the layer it supports. In this respect, the layer encapsulates the data from the supported layer. In the Internet suite of protocols, for example, a packet would contain control information from the physical layer, followed by control information from the network layer, followed by the application protocol data. (2) See also *data link switching*.

encode. To convert data by the use of a code in such a manner that reconversion to the original form is possible. (T)

end node (EN). (1) See *Advanced Peer-to-Peer Networking (APPN) end node* and *low-entry networking (LEN) end node*. (2) In communications, a node that is frequently attached to a single data link and cannot perform intermediate routing functions.

entry point (EP). In SNA, a type 2.0, type 2.1, type 4, or type 5 node that provides distributed network management support. It sends network management data about itself and the resources it controls to a focal point for centralized processing, and it receives and executes focal-point initiated commands to manage and control its resources.

ESI. End System Identifier, a 6-byte component of an ATM address.

Ethernet. A 10-Mbps baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and delayed retransmission. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD).

exception. An abnormal condition such as an I/O error encountered in processing a data set or a file.

exception response (ER). In SNA, a protocol requested in the form-of-response-requested field of a request header that directs the receiver to return a response only if the request is unacceptable as received or cannot be processed; that is, a negative response, but not a positive response, can be returned. Contrast with *definite response* and *no response*.

exchange identification (XID). A specific type of basic link unit that is used to convey node and link characteristics between adjacent nodes. XIDs are exchanged between link stations before and during link activation to establish and negotiate link and node characteristics, and after link activation to communicate changes in these characteristics.

explicit route (ER). In SNA, a series of one or more transmission groups that connect two subarea nodes. An explicit route is identified by an origin subarea address, a destination subarea address, an explicit route number, and a reverse explicit route number. Contrast with *virtual route (VR)*.

explorer frame. See *explorer packet*.

explorer packet. In LANs, a packet that is generated by the source host and that traverses the entire source routing part of a LAN, gathering information on the possible paths available to the host.

exterior gateway. In Internet communications, a gateway on one autonomous system that communicates with another autonomous system. Contrast with *interior gateway*.

Exterior Gateway Protocol (EGP). In the Internet suite of protocols, a protocol, used between domains and autonomous systems, that enables network reachability information to be advertised and exchanged. IP network addresses in one autonomous system are advertised to another autonomous system by means of EGP-participating routers. Contrast with *Border Gateway Protocol (BGP)*.

F

File Transfer Protocol (FTP). In the Internet suite of protocols, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

flow control. (1) In SNA, the process of managing the rate at which data traffic passes between components of the network. The purpose of flow control is to optimize the rate of flow of message units with minimum congestion in the network; that is, to neither overflow the buffers at the receiver or at intermediate routing nodes, nor leave the receiver waiting for more message units. (2) See also *pacing*.

fragment. See *fragmentation*.

fragmentation. (1) The process of dividing a datagram into smaller parts, or fragments, to match the capabilities of the physical medium over which it is to be transmitted. (2) See also *segmenting*.

frame. (1) In Open Systems Interconnection architecture, a data structure pertaining to a particular area of knowledge and consisting of slots that can

accept the values of specific attributes and from which inferences can be drawn by appropriate procedural attachments. (T) (2) The unit of transmission in some local area networks, including the IBM Token-Ring Network. It includes delimiters, control characters, information, and checking characters. (3) In SDLC, the vehicle for every command, every response, and all information that is transmitted using SDLC procedures.

frame level. Synonymous with *data link level*. See *link level*.

Frame Relay. (1) An interface standard describing the boundary between a user's equipment and a fast-packet network. In frame-relay systems, flawed frames are discarded; recovery comes end-to-end rather than hop-by-hop. (2) A technique derived from the integrated services digital network (ISDN) D channel standard. It assumes that connections are reliable and dispenses with the overhead of error detection and control within the network.

G

gateway. (1) A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. (T) (2) In the IBM Token-Ring Network, a device and its associated software that connect a local area network to another local area network or a host that uses different logical link protocols. (3) In TCP/IP, synonym for *router*.

general data stream (GDS). The data stream used for conversations in LU 6.2 sessions.

general data stream (GDS) variable. A type of RU substructure that is preceded by an identifier and a length field and includes either application data, user control data, or SNA-defined control data.

H

header. (1) System-defined control information that precedes user data. (2) The portion of a message that contains control information for the message such as one or more destination fields, name of the originating station, input sequence number, character string indicating the type of message, and priority level for the message.

heap memory. The amount of RAM used to dynamically allocate data structures.

Hello. A protocol used by a group of cooperating, trusting routers to allow them to discover minimal delay routes.

hello message. (1) A message sent periodically to establish and test reachability between routers or between routers and hosts. (2) In the Internet suite of protocols, a message defined by the Hello protocol as an Interior Gateway Protocol (IGP).

heuristic. Pertaining to exploratory methods of problem solving in which solutions are discovered by evaluation of the progress made toward the final result.

high-level data link control (HDLC). In data communication, the use of a specified series of bits to control data links in accordance with the International Standards for HDLC: ISO 3309 Frame Structure and ISO 4335 Elements of Procedures.

hop. (1) In APPN, a portion of a route that has no intermediate nodes. It consists of only a single transmission group connecting adjacent nodes. (2) To the routing layer, the logical distance between two nodes in a network.

hop count. (1) A metric or measure of distance between two points. (2) In Internet communications, the number of routers that a datagram passes through on its way to its destination. (3) In SNA, a measure of the number of links to be traversed in a path to a destination.

host. In the Internet suite of protocols, an end system. The end system can be any workstation; it does not have to be a mainframe.

hysteresis. The amount the temperature must change past the set alert threshold before the alert condition is cleared.

I

I frame. Information frame.

IETF. Internet Engineering Task Force, an organization that produces Internet specifications.

ILMI. Interim Local Management Interface, SNMP-based procedures for managing the User-Network Interface (UNI).

information (I) frame. A frame in I format used for numbered information transfer.

input/output channel. In a data processing system, a functional unit that handles transfer of data between internal and peripheral equipment. (I) (A)

integrated services digital network (ISDN). A digital end-to-end telecommunication network that supports multiple services including, but not limited to, voice and data.

Note: ISDNs are used in public and private network architectures.

interface. (1) A shared boundary between two functional units, defined by functional characteristics,

signal characteristics, or other characteristics, as appropriate. The concept includes the specification of the connection of two devices having different functions. (T) (2) Hardware, software, or both, that links systems, programs, or devices.

interior gateway. In Internet communications, a gateway that communicates only with its own autonomous system. Contrast with *exterior gateway*.

Interior Gateway Protocol (IGP). In the Internet suite of protocols, a protocol used to propagate network reachability and routing information within an autonomous system. Examples of IGPs are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

intermediate node. A node that is at the end of more than one branch. (T)

intermediate session routing (ISR). A type of routing function within an APPN network node that provides session-level flow control and outage reporting for all sessions that pass through the node but whose end points are elsewhere.

International Organization for Standardization (ISO). An organization of national standards bodies from various countries established to promote development of standards to facilitate international exchange of goods and services, and develop cooperation in intellectual, scientific, technological, and economic activity.

International Telecommunication Union (ITU). The specialized telecommunication agency of the United Nations, established to provide standardized communication procedures and practices, including frequency allocation and radio regulations worldwide.

internet. A collection of networks interconnected by a set of routers that allow them to function as a single, large network. See also *Internet*.

Internet. The internet administered by the Internet Architecture Board (IAB), consisting of large national backbone networks and many regional and campus networks all over the world. The Internet uses the Internet suite of protocols.

Internet address. See *IP address*.

Internet Architecture Board (IAB). The technical body that oversees the development of the Internet suite of protocols that are known as TCP/IP.

Internet Control Message Protocol (ICMP). The protocol used to handle errors and control messages in the Internet Protocol (IP) layer. Reports of problems and incorrect datagram destinations are returned to the original datagram source. ICMP is part of the Internet Protocol.

Internet Control Protocol (ICP). The VIrtual NEtworking System (VINES) protocol that provides exception notifications, metric notifications, and PING support. See also *RouTing update Protocol (RTP)*.

Internet Engineering Task Force (IETF). The task force of the Internet Architecture Board (IAB) that is responsible for solving the short-term engineering needs of the Internet.

Internet Protocol (IP). A connectionless protocol that routes data through a network or interconnected networks. IP acts as an intermediary between the higher protocol layers and the physical network. However, this protocol does not provide error recovery and flow control and does not guarantee the reliability of the physical network.

Internetwork Packet Exchange (IPX). (1) The network protocol used to connect Novell's servers, or any workstation or router that implements IPX, with other workstations. Although similar to the Internet Protocol (IP), IPX uses different packet formats and terminology. (2) See also *Xerox Network Systems (XNS)*.

interoperability. The capability to communicate, execute programs, or transfer data among various functional units in a way that requires the user to have little or no knowledge of the unique characteristics of those units. (T)

intra-area routing. In Internet communications, the routing of data within an area.

Inverse Address Resolution Protocol (InARP). In the Internet suite of protocols, the protocol used for locating a protocol address through the known hardware address. In a frame-relay context, the data link connection identifier (DLCI) is synonymous with the known hardware address.

IP address. The 32-bit address defined by the Internet Protocol, standard 5, Request for Comments (RFC) 791. It is usually represented in dotted decimal notation.

IP datagram. In the Internet suite of protocols, the fundamental unit of information transmitted through an internet. It contains source and destination addresses, user data, and control information such as the length of the datagram, the header checksum, and flags indicating whether the datagram can be or has been fragmented.

IP router. A device in an IP internet that is responsible for making decisions about the paths over which network traffic will flow. Routing protocols are used to gain information about the network and to determine the best route over which the datagram should be forwarded toward the final destination. The datagrams are routed based on IP destination addresses.

IPXWAN. A Novell protocol that is used to exchange router-to-router information before exchanging standard Internetwork Packet Exchange (IPX) routing information and traffic over wide area networks (WANs).

L

LAN bridge server (LBS). In the IBM Token-Ring Network Bridge Program, the server that keeps statistical information about frames forwarded between two or more rings (through a bridge). The LBS sends these statistics to the appropriate LAN managers through the LAN reporting mechanism (LRM).

LAN Emulation (LE). An ATM Forum standard that supports legacy LAN applications over ATM networks.

LAN Emulation Client (LEC). A LAN Emulation component that represents users of the Emulated LAN.

LAN Emulation Configuration Server (LECS). A LAN Emulation Service component that centralizes and disseminates configuration data.

LAN Emulation Server (LES). A LAN Emulation Service component that resolves LAN Destinations to ATM Addresses.

LAN Network Manager (LNM). An IBM licensed program that enables a user to manage and monitor LAN resources from a central workstation.

LAN segment. (1) Any portion of a LAN (for example, a bus or ring) that can operate independently, but that is connected to other parts of the network by means of bridges. (2) A ring or bus network without bridges.

layer. (1) In network architecture, a group of services that is complete from a conceptual point of view, that is one out of a set of hierarchically arranged groups, and that extends across all systems that conform to the network architecture. (T) (2) In the Open Systems Interconnection reference model, one of seven conceptually complete, hierarchically arranged groups of services, functions, and protocols, that extend across all open systems. (T) (3) In SNA, a grouping of related functions that are logically separate from the functions in other groups. Implementation of the functions in one layer can be changed without affecting functions in other layers.

LE. LAN Emulation.

LEC. LAN Emulation Client.

LECS. LAN Emulation Configuration Server.

LES. LAN Emulation Server.

line switching. Synonym for *circuit switching*.

link. The combination of the link connection (the transmission medium) and two link stations, one at each end of the link connection. A link connection can be shared among multiple links in a multipoint or token-ring configuration.

link access protocol balanced (LAPB). A protocol used for accessing an X.25 network at the link level. LAPB is a duplex, asynchronous, symmetric protocol, used in point-to-point communication.

link-attached. (1) Pertaining to devices that are connected to a controlling unit by a data link. (2) Contrast with *channel-attached*. (3) Synonymous with *remote*.

link connection. (1) The physical equipment providing two-way communication between one link station and one or more other link stations; for example, a telecommunication line and data circuit-terminating equipment (DCE). (2) In SNA, synonymous with *data circuit*.

link level. (1) A part of Recommendation X.25 that defines the link protocol used to get data into and out of the network across the full-duplex link connecting the subscriber's machine to the network node. LAP and LAPB are the link access protocols recommended by the CCITT. (2) See *data link level*.

link-state. In routing protocols, the advertised information about the usable interfaces and reachable neighbors of a router or network. The protocol's topological database is formed from the collected link-state advertisements.

link station. (1) The hardware and software components within a node representing a connection to an adjacent node over a specific link. For example, if node A is the primary end of a multipoint line that connects to three adjacent nodes, node A will have three link stations representing the connections to the adjacent nodes. (2) See also *adjacent link station (ALS)*.

LIS. Logical IP Subnet, an IP subnet implemented with ATM technology Virtual Networking (SVN) framework.

local. (1) Pertaining to a device accessed directly without use of a telecommunication line. (2) Contrast with *remote*. (3) Synonym for *channel-attached*.

local area network (LAN). (1) A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. (T) (2) A network in which a set of devices are connected to one another for communication and that can be connected to a larger network. (3) See also *Ethernet* and *token ring*. (4) Contrast with *metropolitan area network (MAN)* and *wide area network (WAN)*.

local bridging. A function of a bridge program that allows a single bridge to connect multiple LAN

segments without using a telecommunication link. Contrast with *remote bridging*.

local management interface (LMI). See *local management interface (LMI) protocol*.

local management interface (LMI) protocol. In NCP, a set of frame-relay network management procedures and messages used by adjacent frame-relay nodes to exchange line status information over DLCI X'00'. NCP supports both the American National Standards Institute (ANSI) and International Telegraph and Telephone Consultative Committee (ITU-T/CCITT) versions of LMI protocol. These standards refer to LMI protocol as *link integrity verification tests (LIVT)*.

locally administered address. In a local area network, an adapter address that the user can assign to override the universally administered address. Contrast with *universally administered address*.

logical channel. In packet mode operation, a sending channel and a receiving channel that together are used to send and receive data over a data link at the same time. Several logical channels can be established on the same data link by interleaving the transmission of packets.

logical link. A pair of link stations, one in each of two adjacent nodes, and their underlying link connection, providing a single link-layer connection between the two nodes. Multiple logical links can be distinguished while they share the use of the same physical media connecting two nodes. Examples are 802.2 logical links used on local area network (LAN) facilities and LAP E logical links on the same point-to-point physical link between two nodes. The term logical link also includes the multiple X.25 logical channels that share the use of the access link from a DTE to an X.25 network.

logical link control (LLC). The data link control (DLC) LAN sublayer that provides two types of DLC operation for the orderly exchange of information. The first type is connectionless service, which allows information to be sent and received without establishing a link. The LLC sublayer does not perform error recovery or flow control for connectionless service. The second type is connection-oriented service, which requires establishing a link prior to the exchange of information. Connection-oriented service provides sequenced information transfer, flow control, and error recovery.

logical link control (LLC) protocol. In a local area network, the protocol that governs the exchange of transmission frames between data stations independently of how the transmission medium is shared. (T) The LLC protocol was developed by the IEEE 802 committee and is common to all LAN standards.

logical link control (LLC) protocol data unit. A unit of information exchanged between link stations in different nodes. The LLC protocol data unit contains a destination service access point (DSAP), a source service access point (SSAP), a control field, and user data.

logical unit (LU). A type of network accessible unit that enables users to gain access to network resources and communicate with each other.

loopback test. A test in which signals from a tester are looped at a modem or other network element back to the tester for measurements that determine or verify the quality of the communications path.

low-entry networking (LEN). A capability of nodes to attach directly to one another using basic peer-to-peer protocols to support multiple and parallel sessions between logical units.

low-entry networking (LEN) end node. A LEN node receiving network services from an adjacent APPN network node.

low-entry networking (LEN) node. A node that provides a range of end-user services, attaches directly to other nodes using peer protocols, and derives network services implicitly from an adjacent APPN network node, that is, without the direct use of CP-CP sessions.

M

Management Information Base (MIB). (1) A collection of objects that can be accessed by means of a network management protocol. (2) A definition for management information that specifies the information available from a host or gateway and the operations allowed. (3) In OSI, the conceptual repository of management information within an open system.

management station. In Internet communications, the system responsible for managing all, or a portion of, a network. The management station communicates with network management agents that reside in the managed node by means of a network management protocol, such as the Simple Network Management Protocol (SNMP).

mapping. The process of converting data that is transmitted in one format by the sender into the data format that can be accepted by the receiver.

mask. (1) A pattern of characters used to control retention or elimination of portions of another pattern of characters. (I) (A) (2) To use a pattern of characters to control retention or elimination of portions of another pattern of characters. (I) (A)

maximum transmission unit (MTU). In LANs, the largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the MTU for Ethernet is 1500 bytes.

medium access control (MAC). In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium.

medium access control (MAC) protocol. In a local area network, the protocol that governs access to the transmission medium, taking into account the topological aspects of the network, in order to enable the exchange of data between data stations. (T)

medium access control (MAC) sublayer. In a local area network, the part of the data link layer that applies a medium access method. The MAC sublayer supports topology-dependent functions and uses the services of the physical layer to provide services to the logical link control sublayer. (T)

metric. In Internet communications, a value, associated with a route, which is used to discriminate between multiple exit or entry points to the same autonomous system. The route with the lowest metric is preferred.

metropolitan area network (MAN). A network formed by the interconnection of two or more networks which may operate at higher speed than those networks, may cross administrative boundaries, and may use multiple access methods. (T) Contrast with *local area network (LAN)* and *wide area network (WAN)*.

MIB object. Synonym for *MIB variable*.

MIB variable. In the Simple Network Management Protocol (SNMP), a specific instance of data defined in a MIB module. Synonymous with *MIB object*.

MIB view. In the Simple Network Management Protocol (SNMP), the collection of managed objects, known to the agent, that is visible to a particular community.

MILNET. The military network that was originally part of ARPANET. It was partitioned from ARPANET in 1984. MILNET provides a reliable network service for military installations.

modem (modulator/demodulator). (1) A functional unit that modulates and demodulates signals. One of the functions of a modem is to enable digital data to be transmitted over analog transmission facilities. (T) (A) (2) A device that converts digital data from a computer to an analog signal that can be transmitted on a telecommunication line, and converts the analog signal received to data for the computer.

modulo. (1) Pertaining to a modulus; for example, 9 is equivalent to 4 modulo 5. (2) See also *modulus*.

modulus. A number, such as a positive integer, in a relationship that divides the difference between two related numbers without leaving a remainder; for example, 9 and 4 have a modulus of 5 (9 - 4 = 5; 4 - 9 = -5; and 5 divides both 5 and -5 without leaving a remainder).

monitor. (1) A device that observes and records selected activities within a data processing system for analysis. Possible uses are to indicate significant departure from the norm, or to determine levels of utilization of particular functional units. (T) (2) Software or hardware that observes, supervises, controls, or verifies operations of a system. (A) (3) The function required to initiate the transmission of a token on the ring and to provide soft-error recovery in case of lost tokens, circulating frames, or other difficulties. The capability is present in all ring stations.

MSS. Multiprotocol Switched Services, a component of IBM's Switched Virtual Networking (SVN) framework.

multicast. (1) Transmission of the same data to a selected group of destinations. (T) (2) A special form of broadcast in which copies of a packet are delivered to only a subset of all possible destinations.

multiple-domain support (MDS). A technique for transporting management services data between management services function sets over LU-LU and CP-CP sessions. See also *multiple-domain support message unit (MDS-MU)*.

multiple-domain support message unit (MDS-MU). The message unit that contains management services data and flows between management services function sets over the LU-LU and CP-CP sessions used by multiple-domain support. This message unit, as well as the actual management services data that it contains, is in general data stream (GDS) format. See also *control point management services unit (CP-MSU)*, *management services unit (MSU)*, and *network management vector transport (NMVT)*.

N

Name Binding Protocol (NBP). In AppleTalk networks, a protocol that provides name translation function from the AppleTalk entity (resource) name (character string) into an AppleTalk IP address (16-bit number) on the transport layer.

name resolution. In Internet communications, the process of mapping a machine name to the corresponding Internet Protocol (IP) address. See also *Domain Name System (DNS)*.

name server. In the Internet suite of protocols, synonym for *domain name server*.

nearest active upstream neighbor (NAUN). In the IBM Token-Ring Network, the station sending data directly to a given station on the ring.

neighbor. A router on a common subnetwork that has been designated by a network administrator to receive routing information.

NetBIOS. Network Basic Input/Output System. A standard interface to networks, IBM personal computers (PCs), and compatible PCs, that is used on LANs to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not need to handle the details of LAN data link control (DLC) protocols.

network. (1) A configuration of data processing devices and software connected for information interchange. (2) A group of nodes and the links interconnecting them.

network accessible unit (NAU). A logical unit (LU), physical unit (PU), control point (CP), or system services control point (SSCP). It is the origin or the destination of information transmitted by the path control network. Synonymous with *network addressable unit*.

network address. According to ISO 7498-3, a name, unambiguous within the OSI environment, that identifies a set of network service access points.

network addressable unit (NAU). Synonym for *network accessible unit*.

network architecture. The logical structure and operating principles of a computer network. (T)

Note: The operating principles of a network include those of services, functions, and protocols.

network congestion. An undesirable overload condition caused by traffic in excess of what a network can handle.

network identifier. (1) In TCP/IP, that part of the IP address that defines a network. The length of the network ID depends on the type of network class (A, B, or C). (2) A 1- to 8-byte customer-selected name or an 8-byte IBM-registered name that uniquely identifies a specific subnetwork.

Network Information Center (NIC). In Internet communications, local, regional, and national groups throughout the world who provide assistance, documentation, training, and other services to users.

network layer. In Open Systems Interconnection (OSI) architecture, the layer that is responsible for routing, switching, and link-layer access across the OSI environment.

network management. The process of planning, organizing, and controlling a communication-oriented data processing or information system.

network management station. In the Simple Network Management Protocol (SNMP), a station that executes management application programs that monitor and control network elements.

network management vector transport (NMVT). A management services request/response unit (RU) that flows over an active session between physical unit management services and control point management services (SSCP-PU session).

network manager. A program or group of programs that is used to monitor, manage, and diagnose the problems of a network.

network node (NN). See *Advanced Peer-to-Peer Networking (APPN) network node*.

Next Hop Resolution Protocol (NHRP). A routing protocol, specified in Internet Draft Version 10 which has been submitted for RFC status. The Next Hop Resolution Protocol defines a method for a source station to determine the Non-Broadcast Multi-Access (NBMA) address of the “NBMA next hop” towards a destination. The NBMA next hop may be the destination itself or the router in the NBMA network that is “nearest” to the destination. The source station can then establish an NBMA virtual circuit directly with the destination or the router and reduce the number of routing hops through the NBMA network.

network user address (NUA). In X.25 communications, the X.121 address containing up to 15 binary code digits.

NHRP. Next Hop Resolution Protocol

node. (1) In a network, a point at which one or more functional units connect channels or data circuits. (I) (2) Any device, attached to a network, that transmits and receives data.

noncanonical address. In LANs, a format for the transmission of medium access control (MAC) addresses for token-ring adapters. In noncanonical format, the most significant (leftmost) bit of each address byte is transmitted first. Contrast with *canonical address*.

nonseed router. In AppleTalk networks, a router that acquires network number range and zone list information from a seed router attached to the same network.

O

Open Shortest Path First (OSPF). In the Internet suite of protocols, a function that provides intradomain

information transfer. An alternative to the Routing Information Protocol (RIP), OSPF allows the lowest-cost routing and handles routing in large regional or corporate networks.

Open Systems Interconnection (OSI). (1) The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information. (T) (A) (2) The use of standardized procedures to enable the interconnection of data processing systems.

Note: OSI architecture establishes a framework for coordinating the development of current and future standards for the interconnection of computer systems. Network functions are divided into seven layers. Each layer represents a group of related data processing and communication functions that can be carried out in a standard way to support different applications.

Open Systems Interconnection (OSI) architecture. Network architecture that adheres to that particular set of ISO standards that relates to Open Systems Interconnection. (T)

Open Systems Interconnection (OSI) reference model. A model that describes the general principles of the Open Systems Interconnection, as well as the purpose and the hierarchical arrangement of its seven layers. (T)

origin. An external logical unit (LU) or application program from which a message or other data originates. See also *destination*.

orphan circuit. A non-configured circuit whose availability is learned dynamically.

P

pacing. (1) A technique by which a receiving component controls the rate of transmission of a sending component to prevent overrun or congestion. (2) See also *flow control*, *receive pacing*, *send pacing*, *session-level pacing*, and *virtual route (VR) pacing*.

packet. In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals, and, possibly, error control information are arranged in a specific format. (I)

packet internet groper (PING). (1) In Internet communications, a program used in TCP/IP networks to test the ability to reach destinations by sending the destinations an Internet Control Message Protocol (ICMP) echo request and waiting for a reply. (2) In communications, a test of reachability.

packet mode operation. Synonym for *packet switching*.

packet switching. (1) The process of routing and transferring data by means of addressed packets so that a channel is occupied only during transmission of a packet. On completion of the transmission, the channel is made available for transfer of other packets. (I) (2) Synonymous with *packet mode operation*. See also *circuit switching*.

parallel bridges. A pair of bridges connected to the same LAN segment, creating redundant paths to the segment.

parallel transmission groups. Multiple transmission groups between adjacent nodes, with each group having a distinct transmission group number.

path. (1) In a network, any route between any two nodes. A path may include more than one branch. (T) (2) The series of transport network components (path control and data link control) that are traversed by the information exchanged between two network accessible units. See also *explicit route (ER)*, *route extension*, and *virtual route (VR)*.

path control (PC). The function that routes message units between network accessible units in the network and provides the paths between them. It converts the basic information units (BIUs) from transmission control (possibly segmenting them) into path information units (PIUs) and exchanges basic transmission units containing one or more PIUs with data link control. Path control differs by node type: some nodes (APPN nodes, for example) use locally generated session identifiers for routing, and others (subarea nodes) use network addresses for routing.

path cost. In link-state routing protocols, the sum of the link costs along the path between two nodes or networks.

path information unit (PIU). A message unit consisting of a transmission header (TH) alone, or a TH followed by a basic information unit (BIU) or a BIU segment.

pattern-matching character. A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace a pattern-matching character. Synonymous with *global character* and *wildcard character*.

permanent virtual circuit (PVC). In X.25 and frame-relay communications, a virtual circuit that has a logical channel permanently assigned to it at each data terminal equipment (DTE). Call-establishment protocols are not required. Contrast with *switched virtual circuit (SVC)*.

physical circuit. A circuit established without multiplexing. See also *data circuit*. Contrast with *virtual circuit*.

physical layer. In the Open Systems Interconnection reference model, the layer that provides the mechanical, electrical, functional, and procedural means to establish, maintain, and release physical connections over the transmission medium. (T)

physical unit (PU). (1) The component that manages and monitors the resources (such as attached links and adjacent link stations) associated with a node, as requested by an SSCP via an SSCP-PU session. An SSCP activates a session with the physical unit in order to indirectly manage, through the PU, resources of the node such as attached links. This term applies to type 2.0, type 4, and type 5 nodes only. (2) See also *peripheral PU* and *subarea PU*.

ping command. The command that sends an Internet Control Message Protocol (ICMP) echo-request packet to a gateway, router, or host with the expectation of receiving a reply.

Point-to-Point Protocol (PPP). A protocol that provides a method for encapsulating and transmitting packets over serial point-to-point links.

polling. (1) On a multipoint connection or a point-to-point connection, the process whereby data stations are invited, one at a time, to transmit. (I) (2) Interrogation of devices for such purposes as to avoid contention, to determine operational status, or to determine readiness to send or receive data. (A)

port. (1) An access point for data entry or exit. (2) A connector on a device to which cables for other devices such as display stations and printers are attached. (3) The representation of a physical connection to the link hardware. A port is sometimes referred to as an adapter; however, there can be more than one port on an adapter. There may be one or more ports controlled by a single DLC process. (4) In the Internet suite of protocols, a 16-bit number used to communicate between TCP or the User Datagram Protocol (UDP) and a higher-level protocol or application. Some protocols, such as File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP), use the same well-known port number in all TCP/IP implementations. (5) An abstraction used by transport protocols to distinguish among multiple destinations within a host machine. (6) Synonymous with *socket*.

port number. In Internet communications, the identification of an application entity to the transport service.

problem determination. The process of determining the source of a problem; for example, a program component, machine failure, telecommunication facilities, user or contractor-installed programs or equipment, environmental failure such as a power loss, or user error.

program temporary fix (PTF). A temporary solution or bypass of a problem diagnosed by IBM in a current unaltered release of the program.

protocol. (1) A set of semantic and syntactic rules that determine the behavior of functional units in achieving communication. (I) (2) In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. (T) (3) In SNA, the meanings of, and the sequencing rules for, requests and responses used for managing the network, transferring data, and synchronizing the states of network components. Synonymous with *line control discipline* and *line discipline*. See *bracket protocol* and *link protocol*.

protocol data unit (PDU). A unit of data specified in a protocol of a given layer and consisting of protocol control information of this layer, and possibly user data of this layer. (T)

Q

Quality of Service (QoS). The user-oriented performance of an end-to-end service which is accessed using performance parameters. In ATM networks, the following performance parameters determine the QoS of an end-to-end ATM connection: cell loss ratio, cell transfer delay, and cell delay variation.

R

Rapid Transport Protocol (RTP) connection. In high-performance routing (HPR), the connection established between the endpoints of the route to transport session traffic.

reachability. The ability of a node or a resource to communicate with another node or resource.

read-only memory (ROM). Memory in which stored data cannot be modified by the user except under special conditions.

reassembly. In communications, the process of putting segmented packets back together after they have been received.

receive not ready (RNR). In communications, a data link command or response that indicates a temporary condition of being unable to accept incoming frames.

receive not ready (RNR) packet. See *RNR packet*.

received line signal detector (RLSD). In the EIA 232 standard, a signal that indicates to the data terminal

equipment (DTE) that it is receiving a signal from the remote data circuit-terminating equipment (DCE). Synonymous with *carrier detect* and *data carrier detect (DCD)*.

Recognized Private Operating Agency (RPOA). Any individual, company, or corporation, other than a government department or service, that operates a telecommunication service and is subject to the obligations undertaken in the Convention of the International Telecommunication Union and in the Regulations; for example, a communication common carrier.

reduced instruction-set computer (RISC). A computer that uses a small, simplified set of frequently used instructions for rapid execution.

remote. (1) Pertaining to a system, program, or device that is accessed through a telecommunication line. (2) Synonym for *link-attached*. (3) Contrast with *local*.

remote bridging. The function of a bridge that allows two bridges to connect multiple LANs using a telecommunication link. Contrast with *local bridging*.

Remote Execution Protocol (REXEC). A protocol that allows the execution of a command or program on any host in the network. The local host receives the results of the command execution.

Request for Comments (RFC). In Internet communications, the document series that describes a part of the Internet suite of protocols and related experiments. All Internet standards are documented as RFCs.

reset. On a virtual circuit, reinitialization of data flow control. At reset, all data in transit are eliminated.

reset request packet. In X.25 communications, a packet transmitted by the data terminal equipment (DTE) to the data circuit-terminating equipment (DCE) to request that a virtual call or a permanent virtual circuit be reset. The reason for the request can also be specified in the packet.

ring. See *ring network*.

ring network. (1) A network in which every node has exactly two branches connected to it and in which there are exactly two paths between any two nodes. (T) (2) A network configuration in which devices are connected by unidirectional transmission links to form a closed path.

ring segment. A section of a ring that can be isolated (by unplugging connectors) from the rest of the ring. See *LAN segment*.

rlogin (remote login). A service, offered by Berkeley UNIX-based systems, that allows authorized users of one machine to connect to other UNIX systems across an internet and interact as if their terminals were connected directly. The rlogin software passes information about the user's environment (for example, terminal type) to the remote machine.

RNR packet. A packet used by a data terminal equipment (DTE) or by a data circuit-terminating equipment (DCE) to indicate a temporary inability to accept additional packets for a virtual call or permanent virtual circuit.

root bridge. The bridge that is the root of a spanning tree formed between other active bridges in the bridging network. The root bridge originates and transmits bridge protocol data units (BPDUs) to other active bridges to maintain the spanning tree topology. It is the bridge with the highest priority in the network.

route. (1) An ordered sequence of nodes and transmission groups (TGs) that represent a path from an origin node to a destination node traversed by the traffic exchanged between them. (2) The path that network traffic uses to get from source to destination.

route bridge. A function of an IBM bridge program that allows two bridge computers to use a telecommunication link to connect two LANs. Each bridge computer is connected directly to one of the LANs, and the telecommunication link connects the two bridge computers.

route extension (REX). In SNA, the path control network components, including a peripheral link, that make up the portion of a path between a subarea node and a network addressable unit (NAU) in an adjacent peripheral node. See also *explicit route (ER)*, *path*, and *virtual route (VR)*.

Route Selection control vector (RSCV). A control vector that describes a route within an APPN network. The RSCV consists of an ordered sequence of control vectors that identify the TGs and nodes that make up the path from an origin node to a destination node.

router. (1) A computer that determines the path of network traffic flow. The path selection is made from several paths based on information obtained from specific protocols, algorithms that attempt to identify the shortest or best path, and other criteria such as metrics or protocol-specific destination addresses. (2) An attaching device that connects two LAN segments, which use similar or different architectures, at the reference model network layer. (3) In OSI terminology, a function that determines a path by which an entity can be reached. (4) In TCP/IP, synonymous with *gateway*. (5) Contrast with *bridge*.

routing. (1) The assignment of the path by which a message is to reach its destination. (2) In SNA, the forwarding of a message unit along a particular path through a network, as determined by parameters carried in the message unit, such as the destination network address in a transmission header.

routing domain. In Internet communications, a group of intermediate systems that use a routing protocol so that the representation of the overall network is the same within each intermediate system. Routing domains are connected to each other by exterior links.

Routing Information Protocol (RIP). In the Internet suite of protocols, an interior gateway protocol used to exchange intradomain routing information and to determine optimum routes between internet hosts. RIP determines optimum routes on the basis of route metrics, not link transmission speed.

routing loop. A situation that occurs when routers circulate information among themselves until convergence occurs or until the networks involved are considered unreachable.

routing protocol. A technique used by a router to find other routers and to remain up to date about the best way to get to reachable networks.

routing table. A collection of routes used to direct datagram forwarding or to establish a connection. The information is passed among routers to identify network topology and destination feasibility.

Routing Table Maintenance Protocol (RTMP). In AppleTalk networks, a protocol that provides routing information generation and maintenance on the transport layer by means of the AppleTalk routing table. The AppleTalk routing table directs packet transmission through the internet from source socket to destination socket.

RouTing update Protocol (RTP). The VIrtual NEtworking System (VINES) protocol that maintains the routing database and allows the exchange of routing information between VINES nodes. See also *Internet Control Protocol (ICP)*.

rsh. A variant of the rlogin command that invokes a command interpreter on a remote UNIX machine and passes the command-line arguments to the command interpreter, skipping the login step completely.

S

SDU. Service Data Unit, data as it appears at the interface between a layer and the layer immediately above.

seed router. In AppleTalk networks, a router that maintains configuration data (network range numbers and zone lists, for example) for the network. Each network must have at least one seed router. The seed router must be initially set up using the configurator tool. Contrast with *nonseed router.*

segment. (1) A section of cable between components or devices. A segment may consist of a single patch cable, several patch cables that are connected, or a combination of building cable and patch cables that are connected. (2) In Internet communications, the unit of transfer between TCP functions in different machines. Each segment contains control and data fields; the current byte-stream position and actual data bytes are identified along with a checksum to validate received data.

segmenting. In OSI, a function performed by a layer to map one protocol data unit (PDU) from the layer it supports into multiple PDUs.

sequence number. In communications, a number assigned to a particular frame or packet to control the transmission flow and receipt of data.

server. A functional unit that provides shared services to workstations over a network; for example, a file server, a print server, a mail server. (T)

service access point (SAP). (1) In Open Systems Interconnection (OSI) architecture, the point at which the services of a layer are provided by an entity of that layer to an entity of the next higher layer. (T) (2) A logical point made available by an adapter where information can be received and transmitted. A single service access point can have many links terminating in it.

Service Advertising Protocol (SAP). In Internetwork Packet Exchange (IPX), a protocol that provides the following:

- A mechanism that allows IPX servers on an internet to advertise their services by name and type. Servers using this protocol have their name, service type, and IP address recorded in all file servers running NetWare.
- A mechanism that allows a workstation to broadcast a query to discover the identities of all servers of all types, all servers of a specific type, or the nearest server of a specific type.
- A mechanism that allows a workstation to query any file server running NetWare to discover the names and addresses of all servers of a specific type.

session. (1) In network architecture, for the purpose of data communication between functional units, all the activities which take place during the establishment, maintenance, and release of the connection. (T) (2) A logical connection between two network accessible units (NAUs) that can be activated, tailored to provide various protocols, and deactivated, as requested. Each session is uniquely identified in a transmission header (TH) accompanying any transmissions exchanged during the session.

Simple Network Management Protocol (SNMP). In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol.

Information on devices managed is defined and stored in the application's Management Information Base (MIB).

SLIP. Serial Line IP, an IETF standard for running IP over serial communication links.

SNA management services (SNA/MS). The services provided to assist in management of SNA networks.

SNAP. (1) SubNetwork Access Protocol. (2) SubNetwork Attachment Point.

socket. An endpoint for communication between processes or application programs.

source route bridging. In LANs, a bridging method that uses the routing information field in the IEEE 802.5 medium access control (MAC) header of a frame to determine which rings or token-ring segments the frame must transit. The routing information field is inserted into the MAC header by the source node. The information in the routing information field is derived from explorer packets generated by the source host.

source routing. In LANs, a method by which the sending station determines the route the frame will follow and includes the routing information with the frame. Bridges then read the routing information to determine whether they should forward the frame.

source service access point (SSAP). In SNA and TCP/IP, a logical address that allows a system to send data to a remote device from the appropriate communications support. Contrast with *destination service access point (DSAP)*.

spanning tree. In LAN contexts, the method by which bridges automatically develop a routing table and update that table in response to changing topology to ensure that there is only one route between any two LANs in the bridged network. This method prevents packet looping, where a packet returns in a circuitous route back to the sending router.

sphere of control (SOC). The set of control point domains served by a single management services focal point.

sphere of control (SOC) node. A node directly in the sphere of control of a focal point. A SOC node has exchanged management services capabilities with its focal point. An APPN end node can be a SOC node if it supports the function to exchange management services capabilities.

split horizon. A technique for minimizing the time to achieve network convergence. A router records the interface over which it received a particular route and does not propagate its information about the route back over the same interface.

spoofing. For data links, a technique in which a protocol initiated from an end station is acknowledged and processed by an intermediate node on behalf of the final destination. In IBM 6611 data link switching, for example, SNA frames are encapsulated into TCP/IP packets for transport across a non-SNA wide area network, unpacked by another IBM 6611, and passed to the final destination. A benefit of spoofing is the prevention of end-to-end session timeouts.

standard MIB. In the Simple Network Management Protocol (SNMP), a MIB module that is located under the management branch of the Structure of Management Information (SMI) and that is considered a standard by the Internet Engineering Task Force (IETF).

static route. The route between hosts, networks, or both that is manually entered into a routing table.

station. An input or output point of a system that uses telecommunication facilities; for example, one or more systems, computers, terminals, devices, and associated programs at a particular location that can send or receive data over a telecommunication line.

StreetTalk. In the VIrtual NEtworking System (VINES), a unique network-wide naming and addressing system that allows users to locate and access any resource on the network without knowing the network topology. See also *Internet Control Protocol (ICP)* and *RouTing update Protocol (RTP)*.

Structure of Management Information (SMI). (1) In the Simple Network Management Protocol (SNMP), the rules used to define the objects that can be accessed by means of a network management protocol. (2) In OSI, the set of standards relating to management information. The set includes the *Management Information Model* and the *Guidelines for the Definition of Managed Objects*

subarea. A portion of the SNA network consisting of a subarea node, attached peripheral nodes, and associated resources. Within a subarea node, all network accessible units (NAUs), links, and adjacent link stations (in attached peripheral or subarea nodes) that are addressable within the subarea share a common subarea address and have distinct element addresses.

subnet. (1) In TCP/IP, a part of a network that is identified by a portion of the IP address. (2) Synonym for *subnetwork*.

subnet address. In Internet communications, an extension to the basic IP addressing scheme where a portion of the host address is interpreted as the local network address.

subnet mask. Synonym for *address mask*.

subnetwork. (1) Any group of nodes that have a set of common characteristics, such as the same network ID. (2) Synonymous with *subnet*.

Subnetwork Access Protocol (SNAP). In LANs, a 5-byte protocol discriminator that identifies the non-IEEE standard protocol family to which a packet belongs. The SNAP value is used to differentiate between protocols that use $AA as their service access point (SAP) value.

SubNetwork Attachment Point (SNAP). An LLC header extension that identifies the protocol type of a frame.

subnetwork mask. Synonym for *address mask*.

subsystem. A secondary or subordinate system, usually capable of operating independently of, or asynchronously with, a controlling system. (T)

SVN. Switched Virtual Networking, the name of IBM's framework for building and managing switch-based networks.

switched virtual circuit (SVC). An X.25 circuit that is dynamically established when needed. The X.25 equivalent of a switched line. Contrast with *permanent virtual circuit (PVC)*.

synchronous. (1) Pertaining to two or more processes that depend upon the occurrence of specific events such as common timing signals. (T) (2) Occurring with a regular or predictable time relationship.

Synchronous Data Link Control (SDLC). (1) A discipline conforming to subsets of the Advanced Data Communication Control Procedures (ADCCP) of the American National Standards Institute (ANSI) and High-level Data Link Control (HDLC) of the International Organization for Standardization, for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex or half-duplex over switched or nonswitched links. The configuration of the link connection may be point-to-point, multipoint, or loop. (I) (2) Contrast with *binary synchronous communication (BSC)*.

SYNTAX. In the Simple Network Management Protocol (SNMP), a clause in the MIB module that defines the abstract data structure that corresponds to a managed object.

system configuration. A process that specifies the devices and programs that form a particular data processing system.

system services control point (SSCP). A component within a subarea network for managing the configuration, coordinating network operator and problem determination requests, and providing directory services and other session services for users of the network. Multiple SSCPs, cooperating as peers with one another, can divide the network into domains of control, with each SSCP having a hierarchical control relationship to the physical units and logical units within its own domain.

Systems Network Architecture (SNA). The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks. The layered structure of SNA allows the ultimate origins and destinations of information, that is, the users, to be independent of and unaffected by the specific SNA network services and facilities used for information exchange.

T

Telnet. In the Internet suite of protocols, a protocol that provides remote terminal connection service. It allows users of one host to log on to a remote host and interact as directly attached terminal users of that host.

threshold. (1) In IBM bridge programs, a value set for the maximum number of frames that are not forwarded across a bridge due to errors, before a "threshold exceeded" occurrence is counted and indicated to network management programs. (2) An initial value from which a counter is decremented to 0, or a value to which a counter is incremented or decremented from an initial value.

throughput class. In packet switching, the speed at which data terminal equipment (DTE) packets travel through the packet switching network.

time to live (TTL). A technique used by best-effort delivery protocols to inhibit endlessly looping packets. The packet is discarded if the TTL counter reaches 0.

timeout. (1) An event that occurs at the end of a predetermined period of time that began at the occurrence of another specified event. (I) (2) A time interval allotted for certain operations to occur; for example, response to polling or addressing before system operation is interrupted and must be restarted.

TLV. Type/Length/Value, a generalized information element in a LAN Emulation packet.

token. (1) In a local area network, the symbol of authority passed successively from one data station to another to indicate the station temporarily in control of the transmission medium. Each data station has an opportunity to acquire and use the token to control the medium. A token is a particular message or bit pattern that signifies permission to transmit. (T) (2) In LANs, a sequence of bits passed from one device to another along the transmission medium. When the token has data appended to it, it becomes a frame.

token ring. (1) According to IEEE 802.5, network technology that controls media access by passing a

token (special packet or frame) between media-attached stations. (2) A FDDI or IEEE 802.5 network with a ring topology that passes tokens from one attaching ring station (node) to another. (3) See also *local area network (LAN)*.

token-ring network. (1) A ring network that allows unidirectional data transmission between data stations, by a token passing procedure, such that the transmitted data return to the transmitting station. (T) (2) A network that uses a ring topology, in which tokens are passed in a circuit from node to node. A node that is ready to send can capture the token and insert data for transmission.

topology. In communications, the physical or logical arrangement of nodes in a network, especially the relationships among nodes and the links between them.

topology database update (TDU). A message about a new or changed link or node that is broadcast among APPN network nodes to maintain the network topology database, which is fully replicated in each network node. A TDU contains information that identifies the following:

- The sending node
- The node and link characteristics of various resources in the network
- The sequence number of the most recent update for each of the resources described.

trace. (1) A record of the execution of a computer program. It exhibits the sequences in which the instructions were executed. (A) (2) For data links, a record of the frames and bytes transmitted or received.

transceiver (transmitter-receiver). In LANs, a physical device that connects a host interface to a local area network, such as Ethernet. Ethernet transceivers contain electronics that apply signals to the cable and that sense collisions.

Transmission Control Protocol (TCP). A communications protocol used in the Internet and in any network that follows the U.S. Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It uses the Internet Protocol (IP) as the underlying protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks.

transmission group (TG). (1) A connection between adjacent nodes that is identified by a transmission group number. (2) In a subarea network, a single link or a group of links between adjacent nodes. When a transmission group consists of a group of links, the links are viewed as a single logical link, and the transmission group is called a *multilink transmission group (MLTG)*. A *mixed-media multilink transmission group (MMMLTG)* is one that contains links of different medium types (for example, token-ring, switched SDLC, nonswitched SDLC, and frame-relay links). (3) In an APPN network, a single link between adjacent nodes. (4) See also *parallel transmission groups*.

transmission header (TH). Control information, optionally followed by a basic information unit (BIU) or a BIU segment, that is created and used by path control to route message units and to control their flow within the network. See also *path information unit*.

transparent bridging. In LANs, a method for tying individual local area networks together through the medium access control (MAC) level. A transparent bridge stores the tables that contain MAC addresses so that frames seen by the bridge can be forwarded to another LAN if the tables indicate to do so.

transport layer. In the Open Systems Interconnection reference model, the layer that provides a reliable end-to-end data transfer service. There may be relay open systems in the path. (T) See also *Open Systems Interconnection reference model*.

trap. In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

tunneling. To treat a transport network as though it were a single communication link or LAN. See also *encapsulation*.

T1. In the United States, a 1.544-Mbps public access line. It is available in twenty-four 64-Kbps channels. The European version (E1) transmits 2.048 Mbps. The Japanese version (J1) transmits 1.544 Mbps.

U

UNI. User-Network Interface, the interface between user equipment and an ATM switch network.

universally administered address. In a local area network, the address permanently encoded in an adapter at the time of manufacture. All universally administered addresses are unique. Contrast with *locally administered address*.

User Datagram Protocol (UDP). In the Internet suite of protocols, a protocol that provides unreliable, connectionless datagram service. It enables an application program on one machine or process to send a datagram to an application program on another machine or process. UDP uses the Internet Protocol (IP) to deliver datagrams.

V

V.24. In data communication, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE).

V.25. In data communication, a specification of the CCITT that defines the automatic answering equipment and parallel automatic calling equipment on the General Switched Telephone Network, including procedures for disabling of echo controlled devices for both manually and automatically established calls.

V.35. In data communication, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at various data rates.

V.36. In data communication, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at rates of 48, 56, 64, or 72 kilobits per second.

VCC. Virtual Channel Connection, a connection between parties.

VINES. VIrtual NEtworking System.

virtual circuit. (1) In packet switching, the facilities provided by a network that give the appearance to the user of an actual connection. (T) See also *data circuit*. Contrast with *physical circuit*. (2) A logical connection established between two DTEs.

virtual link. In Open Shortest Path First (OSPF), a point-to-point interface that connects border routers that are separated by a non-backbone transit area. Because area routers are part of the OSPF backbone, the virtual link connects the backbone. The virtual links ensure that the OSPF backbone does not become discontinuous.

Virtual Local Area Network (VLAN). A logical grouping of one or more LANs based on protocol and subnet and used to isolate network traffic within these groups.

VIrtual NEtworking System (VINES). The network operating system and network software from Banyan Systems, Inc. In a VINES network, virtual linking allows all devices and services to appear to be directly connected to each other, when they may actually be thousands of miles apart. See also *StreetTalk*.

virtual route (VR). (1) In SNA, either (a) a logical connection between two subarea nodes that is physically realized as a particular explicit route or (b) a logical connection that is contained wholly within a subarea node for intranode sessions. A virtual route between distinct subarea nodes imposes a transmission priority on the underlying explicit route, provides flow control through virtual route pacing, and provides data integrity through sequence numbering of path information units (PIUs). (2) Contrast with *explicit route (ER)*. See also *path* and *route extension (REX)*.

W

wide area network (WAN). (1) A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. (T) (2) A data communication network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. (3) Contrast with *local area network (LAN)* and *metropolitan area network (MAN)*.

wildcard character. Synonym for *pattern-matching character*.

X

X.21. An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for a general-purpose interface between data terminal equipment and data circuit-terminating equipment for synchronous operations on a public data network.

X.25. (1) An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for the interface between data terminal equipment and packet-switched data networks. (2) See also *packet switching*.

Xerox Network Systems (XNS). The suite of internet protocols developed by the Xerox Corporation. Although similar to TCP/IP protocols, XNS uses different packet formats and terminology. See also *Internetwork Packet Exchange (IPX)*.

Z

zone. In AppleTalk networks, a subset of nodes within an internet.

Zone Information Protocol (ZIP). In AppleTalk networks, a protocol that provides zone management service by maintaining a mapping of the zone names and network numbers across the internet on the session layer.

zone information table (ZIT). A listing of network numbers and their associated zone name mappings in the internet. This listing is maintained by each internet router in an AppleTalk internet.

Index

A

accept-qos-parms-from-lecs
  QoS 478
access
  local connection 47
  physical 47
  remote connection 47
access code of the Voice/Data/Fax Modem 70
access-control
  LECS configuration command 374, 380
  LECS monitoring command 443, 453
Access control configuration commands
  add 381
  disable 381
  enable 381
  list 381
access control configuration commands
  list 453
Access control configuration commands
  remove 382
access control monitoring commands
  create 453
  delete 453
  statistics 454
accessing
  change management
    accessing 115
    summary 115
  protocol
    configuration process 18
    operating (monitor) process 18
  second-level process 14, 16
activate
  GWCON command 130
activating spare interfaces 130
add
  Access control configuration command 381
  ATM configuration command 269
  ATM Virtual Interface configuration command 275
  Bus filter configuration command 356
  Bus filter monitoring command 405
  Bus police configuration command 362
  Bus police monitoring command 411
  change management configuration command 116
  CONFIG command 93
  ELANs configuration command 382
  ELS configuration command 166
  LECS configuration command 374
  LECS policies configuration command 396
  LES-BUS configuration command 355
  security for ELANs configuration command 398
  SuperELAN configuration command 283
add ELAN to SuperELAN
  Selected SuperELAN configuration command 288
add-user-defined
  LECS database sync configuration command 375
add-via-ilmi
  LECS database sync configuration command 376
address registration in LAN emulation 243
address resolution in LAN emulation 243
addresses, entering
  ATM 255
addresses, SLIP 48
advanced
  ELS configuration command 166
  ELS monitoring command 185
ARP configuration
  config 317
  list 317
  remove 317
  set 317
ATM
  how to enter addresses 255
ATM addresses of LAN emulation components 236
ATM addressing 235
ATM configuration commands
  accessing 267
  add 269
  disable 274
  enable 274
  interface 269
  LE-Client 268
  LE-Services 268
  list 269
  qos 270
  remove 270
  set 270
  summary 268
atm-llc
  ATM monitoring commands 277
ATM LLC monitoring command
  list 281
ATM monitoring command
  se-services 297
ATM monitoring commands
  accessing 276
  atm-llc 277
  interface 277, 278, 281
  le-services 277
  list 278
  summary 277
  trace 279
  wrap 280
ATM network interface
  monitoring 267
  using 255
ATM Virtual Interface configuration commands
  add 275
  list 275
  remove 276
  summary 275
ATM Virtual Interface monitoring commands
  summary 281

© Copyright IBM Corp. 1996, 1998

B

backup configuration 53
bank for operational software images 54
basing configuration
  on existing 12
BCM 246
  Support for IP 247
  Support for IPX
    BCM IPX Server Farm 247
    preventing a LEC from being treated as 247
    static entries 368
  support for NetBIOS 248
    NetBIOS Namesharing 248
  support for Source Route Bridging 248
BCM IPX Server Farm
  preventing a LEC from being treated as 247, 368
benefits of LAN emulation 233
boot
  CONFIG command 94
Boot CONFIG
  process
    entering from CONFIG 94
boot config, TFTP file transfer in 55
Boot CONFIG commands
  timedload 125
boot configuration commands 54
boot configuration database
  displaying 121
bridging, configuring using quick configuration 496
bridging option of the Web browser interface 65
Broadcast and Unknown Server 234, 243
broadcast manager 246
  Selected SuperELAN configuration command 288
  Selected SuperELAN monitoring command 299
Broadcast Manager
  Work with SuperELAN monitoring command 298
buffer
  GWCON command 130
BUS 233, 234
  connecting to 243
  functions of 244
bus-filter
  LES-BUS configuration command 355
  LES-BUS monitoring command 404
Bus filter configuration command
  add 356
  disable 359
  enable 359
  remove 360
  set 360
  show 361
Bus filter monitoring command
  add 405
  disable 408
  enable 408
  remove 409
  reset 409
  set 410
  show 410
BUS monitor 251
BUS Police 252
bus-police
  LES-BUS configuration command 361
  LES-BUS monitoring commands 411
Bus police configuration command
  add 362
  remove 362
  set 362
  show 363
Bus police monitoring command
  add 411
  flush 411
  remove 411
  set 412
  show 412
BUS traffic monitoring 364

C

change
  CONFIG command 95
change management 54
  accessing 115
  changing file statuses 55
  commands available from 115
  configuring 115
  copy command 57
  describe load images 56
  disable dumping 56
  enable dumping 56
  managing software files 54
  models 113
  other functions 56
  understanding 113
change management configuration commands
  add 116
  copy 116
  describe 118
  disable 118
  enable 118
  erase 119
  list 121
  lock 121
  set 122
  tftp 123
  unlock 127
clear
  CONFIG command 96
  ELS configuration command 166
  ELS monitoring command 185
  GWCON command 131
  Selected SuperELAN monitoring command 299
Clear counters
  Work with SuperELAN monitoring command 298
clock, setting and changing 111
closing a telnet session 84
command 11
  exit 11
command history 22, 66
command line interface 50
commands
  entering 9

completing the configuration after quick configuration 53
components of LAN emulation 234
config as seen in change management 54
CONFIG commands
  add 93
  boot 94
  change 95
  clear 96
  delete 97
  disable 98
  disable-completion 98
  enable 99
  Enable-completion 99
  event 101
  features 101
  List 102
  load 103
  network 103
  patch 104
  protocol 105
  qconfig 106
  set 106
  summary of 92
  system retrieve 110
  system view 111
  time 111
  unpatch 112
  update 112
  write 112
Config-Only mode
  description 86
  entering automatically 86
  manual entry 86
CONFIG process
  accessing 14
  commands available from 92
  description of 85
  entering 14, 92
  exiting 92
  system dumps 91
configuration
  basing on existing 12
  completing after quick configuration 53
  displaying information about 132
  file, backup 53
  first 11
  GWCON command 132
  initial 52
  managing problems 53
  network interfaces 17
  OPCON command 16, 76
  quick 53
  suggestions 11
  tools 49
  updating 12
  updating memory 112
configuration and console menu of the Web browser interface 61
configuration and monitoring tools 49
configuration commands
  GWCON prompt 19
  set prompt-level
    add prefix to hostname 109
configuration files
  changing status 55
  managing 54
  managing using the Configuration Program 55
  status 54
  viewing 54
configuration option of the Voice/Data/Fax Modem 73
configuration program
  using to manage the configuration files 55
configuration using the Voice/Data/Fax Modem 68
configuration using the Web browser interface 62
configuring
  FDDI 223
  IP 498
  IPX 500
  OPCON 75
  user access 87
configuring spare interfaces 88
  activating 130
  configuring 88
  restrictions 89
connecting to a process 9
connecting to the BUS 243
console
  OPCON command 76
console access, local and remote 51
console monitoring of the Web browser interface 62
copy
  change management configuration command 116
copy command in change management 57
CPU
  displaying memory usage of 136
create
  access control monitoring command 453
  ELAN monitoring command 455
  LAN Emulation Services monitoring command 401
  LECS database sync monitoring command 444
  LECS monitoring command 443
  LECS policies monitoring command 467
  LECS security monitoring command 469
Create
  SE Services monitoring command 297
create
  SE Services monitoring command 297
Create
  Selected SuperELAN monitoring command 299
  Work with SuperELAN monitoring command 298

D

data direct VCCs 245
Data/Fax Modem 50
  configuring 67
  default settings 49
  description 67
Data/Fax Modem support 67

database
LES-BUS monitoring command 413
database-synchronization
LECS configuration command 375
LECS monitoring command 443
date, setting and changing 111
default
ELS configuration command 167
default settings for the serial port and the Data/Fax Modem 49
delete
access control monitoring command 453
CONFIG command 97
ELAN monitoring command 455
ELS configuration command 167
LECS database sync monitoring command 444
LECS monitoring command 445
LECS policies monitoring command 467
LECS security monitoring command 469
LES-BUS monitoring command 421
Delete
Super ELAN configuration command 284
delete ELAN from SuperELAN
Selected SuperELAN configuration command 288
describe
change management configuration command 118
describe load images 56
description of OPCON 75
description of the Data/Fax Modem 67
device presence and status report of the Voice/Data/Fax Modem 73
devices option of the Web browser interface 64
diags
OPCON command 77
disable
Access control configuration command 381
ATM configuration command 274
Bus filter configuration command 359
Bus filter monitoring command 408
change management configuration command 118
CONFIG command 98
GWCON command 134
LECS database sync configuration command 376
LECS policies configuration command 397
LES-BUS configuration command 363
LES-BUS monitoring command 421
performance configuration command 214
performance monitoring command 216
security for ELANs configuration command 399
Selected ELAN configuration command 294
Selected ELAN monitoring command 305
Selected SuperELAN configuration command 289
Selected SuperELAN monitoring command 299
Disable
Work with SuperELAN monitoring command 298
disable-completion
CONFIG command 98
disable dumping 56
display
ELS configuration command 167
ELS monitoring command 185
display *(continued)*
Selected ELAN monitoring command 167
Selected SuperELAN monitoring command 300
Display counters
Work with SuperELAN monitoring command 298
display hostname 110
display hostname software VPD 110
display hostname with carriage return 110
display hostname with changes 110
display hostname with date 110
display hostname with time 110
displaying
boot configuration database 121
divert
OPCON command 77
downloading files to the IBM 8210 54
dumping, disabling 56
dumping, enabling 56
duplicate policy values 241
dynamic routing
OSPF 499
RIP 499

E

ELAN details monitoring commands
les 457
list 459
policy 460
set 461
summary of 457
ELAN monitoring commands
create 455
delete 455
list 455
select elan 456
statistics 456
summary of 454
ELAN name policy 240
elan-tlv
ELANs detailed configuration commands 390
ELANs detailed monitoring commands 462
ELAN type policy 241
elans
LECS configuration command 377
LECS monitoring command 445
Selected SuperELAN configuration command 289
Selected SuperELAN monitoring command 300
ELANs
Work with SuperELAN monitoring command 298
ELANs configuration commands
add 382
list 383
remove 383
select 383
summary 382
ELANs configuration commands, detailed
les 384
list 387
policy 387
set 390

ELANs configuration commands, detailed *(continued)*
summary 384
ELANs detailed configuration commands
ELAN-TLV 390
LEC-TLV 394
ELANs detailed monitoring commands
elan-tlv 462
lec-tlv 465
ELS
capturing output using Telnet 150
concepts of 146
description of 145
entering 101
how to use 149
interpreting messages 147
message buffering
overview 161
monitoring 165
els
OPCON command 78
ELS
reloading 194
remote logging
additional considerations 160
duplicate logging 160
messages containing IP addresses 160
output 157
recurring sequence numbers 161
remote-logging 175, 195
setting up traps 151
storing 194
tracing 177, 197
trapping 196, 202
troubleshooting example 1 151
troubleshooting example 2 152
troubleshooting example 3 152
using to troubleshoot 151
ELS (event logging system) monitoring of the Web browser interface 62
ELS configuration
entering and exiting 146
ELS configuration commands
add 166
advanced 166
clear 166
default 167
delete 167
display 167
list 168
message buffering 180
list 180
log 181
nolog 181
set 182
nodisplay 169
noremote 170
notrace 171
notrap 172
remote 173
set 174
summary of 165
ELS configuration commands *(continued)*
trace 166
trap 179
ELS configuration environment
entering and exiting 165
ELS console environment
8210 remote logging
configuration 155
level
defined 153
remote logging 153
remote workstation
configuration 153
syslog facility
defined 153
ELS messages 148
enabling logging to a remote file (Remote) 173, 192
explanation 148
groups 149
logging level 147
managing rotation 150
network information 149
suppressing display of 169
suppressing display of (nodisplay) 189
suppressing remote log (noremote) 170, 189
suppressing tracing 190
suppressing trapping 172, 191
suppressing trapping of (notrap) 191
trace 179
tracing 202
trapping 179, 202
ELS monitoring commands
advanced 185
clear 185
display 185
files 186
list 186
message buffering 207
flush 207
list 208
log 208
nolog 209
read-file 209
set 209
tftp 211
view 211
write-buffer 212
nodisplay 189
noremote 189
notrace 190
notrap 191
remote 192
remove 194
restore 194
retrieve 194
save 194
set 194
statistics 200
summary 184
trap 202
view 203

ELS operating environment
entering and exiting 184
enable
Access control configuration command 381
ATM configuration command 274
Bus filter configuration command 359
Bus filter monitoring command 408
change management configuration command 118
CONFIG command 99
LECS database sync configuration command 376
LECS policies configuration command 397
LES-BUS configuration command 364
LES-BUS monitoring command 423, 424
performance configuration command 214
performance monitoring command 216
security for ELANs configuration command 399
Selected ELAN configuration command 295
Selected ELAN monitoring command 306
Selected SuperELAN configuration command 289
Selected SuperELAN monitoring command 300
Enable
Work with SuperELAN monitoring command 298
Enable-completion
CONFIG command 99
enable dumping 56
encapsulation type 500
end system identifier 235
environment, lower level 11
exiting 11
erase
Change management configuration command 119
error
codes
interpreting hardware 38
GWCON command 134
error codes
hardware 38
ESI 235
Ethernet
encapsulation type 500
encapsulation types for IPX 501
Ethernet configuration commands
ip-encapsulation 318, 331
event
CONFIG command 101
GWCON command 135
OPCON command 78
event logging
subsystem 147
event logging system monitoring of the Web browser interface 62
event logs option of the Voice/Data/Fax Modem 73
event number parameter 147
Events
Causes 146
examples of initial configuration 52
Exit
Work with SuperELAN monitoring command 299
exit command 11
exiting 11
lower level environments 11
exiting the router 6

F

fax accumulation 51
FDDI
configuring 223
GWCON 226
FDDI (Fiber Distributed Data Interface)
using 219
FDDI and GWCON 226
FDDI configuration commands 223
accessing 223
list 223
set 224
FDDI monitoring commands
accessing 225
list 226
SRT-STATS 226
FDDI overview 219
features 101
accessing configuration and console processes 17
bandwidth reservation 135
CONFIG command 101
GWCON command 135
MAC filtering 135
Quality of Service (QoS) 473
WAN restoral 135
Fiber Distributed Data Interface
overview 219
protocols supported 219
file transfer 52
file transfer using TFTP 55
files
ELS monitoring command 186
files, changing status of 55
first
configuration 11
Flow control
packets 131
flush
Bus police monitoring command 411
OPCON command 78
Selected ELAN monitoring command 306
Selected SuperELAN monitoring command 301
Flush
Work with SuperELAN monitoring command 298
forum-compliant LEC
ARP configuration 316
configuring a specific client 315
functions
change management 54
file transfer 52
file transfer using TFTP 55
functions of the BUS 244

G

getting help 10
group
deleting 167
group name parameter 149

guided configuration using the Web browser
interface 63
GWCON
FDDI 226
process
entering 15
GWCON and FDDI 226
GWCON commands
activate 130
buffer 130
clear 131
configuration 132
disable 134
error 134
event 135
features 135
interface 135
memory 136
network 137
protocol 138
queue 139
reset 140
statistics 140
summary of 130
test 140
uptime 141
GWCON process
description of 129
entering and exiting 129

H

halt
OPCON command 78
hardware
error codes 38
help 10
console command 10
Home Page Structure of the Web browser interface 60
how to list the protocols 106
HTML interface 59

I

IBM 8210
Config-Only mode 86
IBM LAN Emulation Client
configuring an Ethernet IBM client 330
identifying prompts 10
ILMI functions in LAN emulation 237
image
loading at specific time 114
image of the operational software 54
Immunity from BUS Police 252
initial configuration 52
examples 52
installing the Voice/Data/Fax Modem 67
intercept
OPCON command 79
intercept character 11
changing 79
interface
ATM configuration command 269
ATM monitoring commands 277, 278, 281
GWCON command 135
list of processes 6
user 6
interface device
adding 93
changing 95
interfaces
configuring spare 88
interfaces, restrictions 89
Interim Local Management Interface 237
IP, configuring 498
IP (Internet Protocol), configuring using quick configuration 498
ip-encapsulation
Ethernet configuration command 318, 331
IP monitoring commands
ping 80
IP option of the Web browser interface 65
IPX, configuring 500
IPX (Internetwork Packet Exchange)
configuring using quick configuration 500
Ethernet encapsulation types 501
token ring encapsulation types 500
IPX option of the Web browser interface 66

K

key parameters for LAN emulation 254

L

LAN destination policy (MAC address policy) 240
LAN emulation 233
address registration to the LES 243
address resolution by the LES 243
addressing in ATM 235
ATM addresses of LAN emulation components 236
ATM addressing for 235
benefits 233
Broadcast and Unknown Server (BUS) 234
Broadcast Manager (BCM) 246
BUS 234
BUS monitor 251
client 234
components 234
components, ATM addresses of 236
configuration of the signaling version 237
configuration server 234
configuration server, policies and policy values 239
connecting to the BUS 243
connecting to the LES 242
ELAN name policy 240
ELAN type policy 241
establishing data direct VCCs 245
functions of the BUS 244
ILMI functions, related 237
key configuration parameters 254
LAN Emulation Configuration Server, overview of 238

LAN emulation 243 *(continued)*
LECS, overview of 243
LECS, policies and policy values 239
LECS duplicate policy values 241
LECS LAN destination policy (MAC address policy) 240
LECS TLVs 241
locating the LECS using ILMI 237
max frame size policy 241
overview 233
overview of related ILMI functions 237
overview of server extensions for LAN emulation 246
redundancy 248
reliability 248
sample assignment policies for LECS 240
security 250
server 234
signaling version 237
LAN Emulation Client (LEC)
configuring 313
LAN Emulation client environment 311
LAN Emulation Configuration Server 238
LAN emulation option of the Web browser interface 64
LAN Emulation Server 242
LAN Emulation Services
components 349
configuration 349
configuration command 352
configuring 351
lecs command 352
les-bus command 352
LAN Emulation Services monitoring commands
accessing 400
create 401
lecs 401
les-bus 401
list 402
security 402
summary 400, 403
work 403
LE client 234
LE-Client
ATM configuration command 268
QoS monitoring command 487
LE-client configuration
Selected SuperELAN configuration command 295
LE-Services
ATM configuration command 268
le-services
ATM monitoring command 277
LE Services configuration command
list 353
rename 353
security 354
lec
Selected ELAN monitoring command 307
LEC monitoring commands
accessing 337
list 339
mib 342
LEC monitoring commands *(continued)*
summary of 337
lec-tlv
ELANs detailed configuration commands 394
ELANs detailed monitoring commands 465
LECS 233
and LAN emulation 234
and LAN extensions 238
component of LAN emulation 238
duplicate policy values 241
ELAN name policy 240
ELAN type policy 241
LAN destination policy (MAC address policy) 240
lecs
LAN Emulation Services monitoring command 401
LE Services configuration command 352
LECS
max frame size policy 241
sample assignment policies 240
TLVs 241
LECS commands
summary of 442
LECS configuration commands
access-control 374, 380
add 374
database-synchronization 375
elans 377
list 378
policies 378
search 378
set 379
summary 374
LECS database sync configuration commands
add-user-defined 375
add-via-ilmi 376
disable 376
enable 376
list 377
remove 377
LECS database sync monitoring commands
create 444
delete 444
list 444
write 445
LECS database synchronization 252
LECS monitoring commands
access-control 443, 453
create 443
database-synchronization 443
delete 445
elans 445
list 445
memory 447
policies 448
restart 448
search 448
set 450
statistics 452
LECS policies configuration commands
add 396
disable 397

LECS policies configuration commands *(continued)*
enable 396
list 397
remove 397
summary 396
LECS policies monitoring commands
create 467
delete 467
list 467
statistics 468
summary of 466
LECS security monitoring commands
create 469
delete 469
list 470
restart 471
statistics 471
summary of 469
LES 233, 234
address registration 243
address resolution 243
connecting to 242
les
ELAN details monitoring command 457
ELANs detailed configuration command 384
les-bus
LAN Emulation Services console command 401
LE Services configuration command 352
Selected SuperELAN configuration command 295
Selected SuperELAN monitoring command 307
LES-BUS configuration command
add 355
bus-filter 355
bus-police 361
BUS traffic monitoring 364
disable 363
enable 364
list 366
remove 366
set 367
set bus-mode 368
summary 354
LES-BUS monitoring commands
bus-filter 404
bus-police 411
database 413
delete 421
disable 421
enable 423, 424
restart 427
set 427
show 429
statistics 431
stop 441
summary of 404
takeover 441
terminate 441
list 18
Access control configuration command 381
access control configuration command 453
ATM configuration command 269
list 281 *(continued)*
ATM LLC monitoring command 381
ATM monitoring commands 278
ATM Virtual Interface configuration command 275
change management configuration command 121
CONFIG command 102
ELAN details monitoring command 459
ELAN monitoring command 455
ELANs configuration command 383
ELANs detailed configuration command 387
ELS configuration command 168
ELS monitoring command 186
LAN Emulation Services monitoring command 402
LE Client QoS configuration commands 480
LE Services configuration command 353
LEC monitoring command 339
LECS configuration command 378
LECS database sync configuration command 377
LECS database sync monitoring command 444
LECS monitoring command 445
LECS policies configuration command 397
LECS policies monitoring command 467
LECS security monitoring command 470
LES-BUS configuration command 366
LLC configuration command 336
LLC monitoring command 347
performance configuration command 214
performance monitoring command 216
List
SE Services monitoring command 297
list
SE Services monitoring command 298
security for ELANs configuration command 399
Selected ELAN configuration command 295
Selected ELAN monitoring command 307
Selected SuperELAN configuration command 290
Selected SuperELAN monitoring command 301
SuperELAN configuration command 284
List
Work with SuperELAN monitoring command 298
list devices 267
list devices command 16, 400
listing the configuration 106
LLC configuration commands
list 336
set 336
summary 336, 347
LLC monitoring commands
list 347
set 347
load
CONFIG command 103
loading
at specific time 114
local consoles 4
local terminals 4
locating the LECS using ILMI 237
lock
change management configuration command 121
lock command in change management 57

logging in
from local console 5
from remote console 5
remote login name 5
login
disabling 98
logout
OPCON command 79

M

MAC address policy (LAN destination policy) 240
maintenance log configuration parameter of the Voice/Data/Fax Modem 70
managing configuration problems 53
managing software files 54
max-burst-size
QoS 476
max frame size policy 239, 241
max-reserved-bandwidth
QoS parameter 474
memory
displaying information about 136
erasing information 194
GWCON command 136
LECS monitoring command 447
obtaining information about 79
OPCON command 79
menu, configuration and console of the Web browser interface 61
menu items of the Voice/Data/Fax Modem 70
message buffering
ELS configuration commands 180
list 180
log 181
nolog 181
set 182
ELS monitoring commands 207
flush 207
list 208
log 208
nolog 209
read-file 209
set 209
tftp 211
view 211
write-buffer 212
overview 161
messages
explanation 148
interpreting 147
receiving 143
messaging process
commands affecting 143
description of 143
entering and exiting 143
OPCON commands 143
receiving messages 143
mib
LEC monitoring command 342
migrate
SuperELAN configuration command 285
monitoring
ATM 267
network interfaces 17
performance monitoring commands 215
monitoring, console of the Web browser interface 62
monitoring, event logging system of the Web browser interface 62
monitoring commands
LAN Emulation Client (LEC) 313
MONITR process
commands affecting 143
description of 143
entering and exiting 143
OPCON commands 143
receiving messages 143
Multiprotocol Switched Services Client Configuration Program 49

N

negotiate-qos
QoS 478
network
CONFIG command 103
environment 103, 137
GWCON command 137
network command 16, 267, 338
network interface
accessing configuration process 16
accessing console process 17
configuring 16
console process 16
deleting 97
disabling 134
displaying information about 102, 132, 135
enabling 140
monitoring 17
supported interfaces 17
verifying 140
network monitoring using the Voice/Data/Fax Modem 68
network software
displaying statistical information about 140
nodisplay
ELS configuration command 169
ELS monitoring command 189
nonvolatile configuration memory
replacing 95
noremote
ELS configuration command 170
ELS monitoring command 189
notrace
ELS configuration command 171
ELS monitoring command 190
notrap
ELS configuration command 172
ELS monitoring command 191

O

obtaining status of telnet session 84
off
  packet trace monitoring command 204
on
  packet trace monitoring command 204
online help 20, 22
OPCON commands
  configuration 76
  console 76
  diags 77
  divert 77
  els 78
  event 78
  flush 78
  halt 78
  intercept 79
  logout 79
  memory 79
  reload 81
  status 81
  summary of 75
  talk 82
  telnet 83
OPCON interface
  configuring 75
OPCON process
  accessing 75
  commands available from 75
  description 75
  getting back to 11
  summary 6
operational software files 52
  changing status 55
  managing 54
  status 54
  viewing 54
OSPF 499
other change management functions 56
output
  discarding 78
  sending to other consoles 77
  suspending 78
overview
  of software 6
overview of LAN emulation 233

P

packet completion codes 148
packet forwarder
  entering CONFIG environment for 105
packet trace
  packet trace monitoring command 192
packet trace messages
  tracing packets 192
packet trace monitoring commands
  off 204
  on 204
  packet Trace 192
  reset 204
packet trace monitoring commands *(continued)*
  set 204
  subsystems 205
  trace-status 206
  view 206
parameter descriptor entries
  QoS 491
parameters
  configuring 106
  event number 147
  for LAN emulation 254
  key LAN emulation 233
password, setting for user 94
passwords 5
patch
  CONFIG command 104
PCMCIA modem 47, 50, 51, 59, 60, 67
peak-cell-rate
  QoS 475
perf command 214
performance
  configuring 213
performance configuration commands
  disable 214
  enable 214
  list 214
  set 215
  summary 214
performance monitoring commands
  accessing 215
  disable 216
  enable 216
  list 216
  report 216
  set 216
  summary of 215
physical access to the 8210 47
pin parameter
  setting 175
ping
  IP monitoring command 80
policies 233
  agreement of 239
  LECS configuration command 378
  LECS monitoring command 448
policies and policy values 239
policy
  ELAN details monitoring command 460
  ELANs detailed configuration command 387
port 49
problems in configuration 53
process
  second-level
    accessing 14, 16
processes
  communicating with 6
  list of 6
prompt-level
  additional functions of
    display hostname with carriage return 110
    display hostname with changes 110

prompt-level *(continued)*
display hostname with date 110
display hostname with time 110
display hostname with VPD 110
configuration command
add prefix to hostname 109
display hostname 110
prompts
CONFIG 10
GWCON 10
identifying 10
OPCON 10
router processes 10
protocol
CONFIG command 105
entering configuration process 18
GWCON command 138
protocol command 18, 19
protocol console process
entering 19
protocols
configuration and console processes
accessing 18
configuring using quick configuration 498
console process 15
displaying information about 132
entering configuration environment for 106
entering console process 19
generating a list of 106

Q

qconfig
CONFIG command 106
QoS
accept-qos-parms-from-lecs 478
accessing configuration prompt 478
accessing monitoring commands 487
ATM configuration command 270
ATM interface configuration commands
Remove 484, 487
Set 485
benefits 473
configuration commands 479
configuration parameters 474
configurations 489
Configuring 473
LE Client configuration commands
List 480
Remove 484
Set 480
LE Client configuration commands, summary 480
LE-Client QoS monitoring command summary 488
LE-Client QoS monitoring commands
List 488
LEC Data Direct VCCs 489
LEC VCC table 491
max-burst-size 476
max-reserved-bandwidth parameter 474
monitoring commands
LE-Client 487
QoS *(continued)*
monitoring commands summary 478
negotiate-qos 478
parameter descriptor entries 491
peak-cell-rate parameter 475
qos-class 476
statistics 490
sustained-cell-rate 475
traffic 491
traffic-type parameter 475
using 473
validate-pcr-of-best-effort-vccs 477
qos-class
QoS 476
Quality of Service 473
queue
GWCON command 139
Quick Config mode 87
manual entry 87
quick configuration 8, 15, 53
bridging configuration 496
description 86
protocol configuration
IP user interface 498
IPX user interface 500
procedure 498
Quick Configuration Reference 495
quick configuration using the Web browser interface 63

R

redundancy of LAN emulation servers 248
reliability of LAN emulation 248
reload 54
OPCON command 6, 81
reloading 15
router 6
remote
ELS configuration command 173
ELS monitoring command 192
remote connection
local connection 47
remote consoles 5
remote logging
additional considerations 160
duplicate logging 160
messages containing IP addresses 160
recurring sequence numbers 161
output examples 157
remote login 5
remote service using the Voice/Data/Fax Modem 68
remote terminals 5
remote voice access 51
remove
Access control configuration command 382
ATM configuration command 270
ATM interface QoS configuration commands 484, 487
ATM Virtual Interface configuration command 276
Bus filter configuration command 360
Bus filter monitoring command 409

remove *(continued)*
Bus police configuration command 382
Bus police monitoring command 411
ELANs configuration command 383
ELS monitoring command 194
LE Client QoS configuration commands 484
LECS database sync configuration command 377
LECS policies configuration command 397
LES-BUS configuration command 366
security for ELANs configuration command 399
rename
LE Services configuration command 353
SuperELAN configuration command 287
report
performance monitoring command 216
reports option of the Voice/Data/Fax Modem 72
resend last Fax report option of the Voice/Data/Fax Modem 74
reset
Bus filter monitoring command 409
GWCON command 140
packet trace monitoring command 204
reset option of the Voice/Data/Fax Modem 71
resetting the IBM 8210 54
restart 54
LECS monitoring command 448
LECS security monitoring command 471
LES-BUS monitoring command 427
Selected ELAN monitoring command 308
Selected SuperELAN monitoring command 302
Restart
Work with SuperELAN monitoring command 298
restarting the IBM 8210 502
restore
ELS monitoring command 194
retrieve
ELS monitoring command 194
RIP 499
route descriptor policy 239
router
deleting configuration information 96
displaying information about 102
displaying time statistics about 141
exiting 6
rebooting 81
reloading 6, 15
router consoles
local 4
remote 5
using 3
router processes
attaching to 83
connecting to 9
displaying information about 81
router software
communicating with 138
reloading 81
user interface 3
Routing and Bridging
SuperELANs 252
rules for using the Web browser interface 59

S

sample, quick configuration 495
save
ELS monitoring commands 194
se-services
ATM monitoring command 297
SE Services monitoring command
Create 297
List 297
list 298
Work with SuperELAN 297
work with SuperELAN 298
search
LECS configuration command 378
LECS monitoring command 448
second-level
process
accessing 14, 16
security
LAN Emulation Services monitoring commands 402
LE Services configuration command 354
security for ELANs configuration commands
add 398
disable 399
enable 399
list 399
remove 399
set 399
summary 398
security of LAN emulation 250
select
ELANs configuration command 383
select elan
ELAN monitoring commands 456
Selected ELAN configuration commands
disable 294
Enable 295
List 295
Spanning Tree port 296
Trace 296
Selected ELAN monitoring commands
disable 305
display 306
enable 306
flush 306
lec 307
list 307
restart 308
show 308
trace 308
Selected SuperELAN configuration commands
Add ELAN to SuperELAN 288
Broadcast Manager 288
Delete ELAN from SuperELAN 288
Disable 289
Elans 289
Enable 289
LE-client configuration 295
LES-BUS 295
List 290
Set 290

Selected SuperELAN configuration commands *(continued)*
Trace 288
Work with ELAN 293
Selected SuperELAN monitoring command
Broadcast Manager 299
clear 299
Create 299
Disable 299
Display 300
ELANs 300
Enable 300
Flush 301
List 301
Restart 302
set cache 302
Show 303
Trace 303
Work with ELAN 304
Selected SuperELAN monitoring commands
LES-BUS 307
Work with SuperELAN monitoring command 298
selector 235
serial port
default settings 49
server extensions for LAN emulation 246
servicing the MSS Server remotely, using the Voice/Data/Fax Modem 68
session
terminating 79
set
ATM configuration command 270
ATM interface QoS configuration commands 485
Bus filter configuration command 360
Bus filter monitoring command 410
Bus police configuration command 362
Bus police monitoring command 412
change management configuration command 122
CONFIG command 106
ELAN details monitoring command 461
ELANs detailed configuration command 390
ELS configuration command 174
ELS monitoring command 194
LE Client QoS configuration commands 480
LECS configuration command 379
LECS monitoring command 450
LES-BUS configuration command 367
LES-BUS monitoring command 427
LLC configuration command 336
LLC monitoring command 347
packet trace monitoring command 205
performance configuration command 215
performance monitoring command 216
security for ELANs configuration command 399
Selected SuperELAN configuration command 290
Set
Work with SuperELAN monitoring command 299
set bus-mode
LES-BUS configuration command 368
set cache
Selected SuperELAN monitoring command 302
setting and changing time, date, and clock 111
setup of the Web browser interface 59
show
Bus filter configuration command 361
Bus filter monitoring command 410
Bus police configuration command 363
Bus police monitoring command 412
LES-BUS monitoring command 429
Selected ELAN monitoring command 308
Selected SuperELAN monitoring command 303
Show cache
Work with SuperELAN monitoring command 299
signaling version configuration in LAN emulation 237
SLIP addresses 48
software
overview 6
user interface 6
spanning tree port
Selected ELAN configuration command 296
SRAM device records
recreating 93
statistics
access control monitoring command 454
clearing 131
ELAN monitoring command 456
ELS monitoring command 200
GWCON command 140
LECS monitoring command 452
LECS policies monitoring command 468
LECS security monitoring command 471
LES-BUS monitoring command 431
QoS 490
status
OPCON command 81
status and statistics option of the Voice/Data/Fax Modem 71
stop
LES-BUS monitoring command 441
subsystems
packet trace monitoring command 205
suggestions
configuration 11
summary
LAN Emulation Services monitoring commands 403
SuperELAN configuration commands
add 283
delete 284
list 284
migrate 285
rename 287
summary 283
vlans 294
work with SuperELAN 287
SuperELAN monitoring commands
vlans 304
SuperELANs 252
sustained-cell-rate
QoS 475
system dumps, using 91
system retrieve
CONFIG command 110

system view
CONFIG command 111

T

takeover
LES-BUS console command 441
talk
OPCON command 82, 213, 215
technical support access 87
telnet
closing a connection 84
obtaining status of Telnet session 84
OPCON command 83
quitting a session 84
telnet command 83
telnet connections 5
closing 84
obtaining status of 84
terminate
LES-BUS console command 441
test
GWCON command 140
tftp
change management configuration command 123
TFTP
description of
related to change management 113
TFTP for file transfer 55
thermal shutdown mode configuration 73
time
activated load of image 114
CONFIG command 111
setting and changing 111
timedload
Boot CONFIG command 125
TLVs
defined on an ELAN basis 241
token ring
encapsulation types for IPX 500
tools for configuration and monitoring 49
trace
ATM monitoring commands 279
ELS configuration commands 202
Selected ELAN configuration command 296
Selected ELAN monitoring command 308
Selected SuperELAN configuration command 292
Selected SuperELAN monitoring command 303
Trace
Work with SuperELAN monitoring command 299
trace-status
packet trace monitoring command 206
traffic-type
QoS parameter 475
trap
ELS configuration commands 179
ELS monitoring command 202
type length values 241

U

unlock
change management configuration command 127
unlock command in change management 57
unpatch
CONFIG command 112
update
CONFIG command 112
updating
configuration 12
uptime
GWCON command 141
user access
adding user 94
changing user 96
configuring 87
deleting user 98
setting password 94
user interface
processes 6
software 6
using the World Wide Web interface 59

V

validate pcr-of-best-effort-vccs
QoS 477
view
ELS monitoring command 203
packet trace monitoring command 206
vlans
SuperELAN configuration command 294
SuperELAN monitoring command 304
VLANs
Work with SuperELAN monitoring command 299
voice access using the Voice/Data/Fax Modem 67
Voice/Data/Fax Modem 50
access code 70
configuration option 73
configuration using 68
configuring 67
device presence and status report 73
event logs 73
installation 67
maintenance log configuration parameter 70
menu items 70
network monitoring using 68
remote service using 68
reports option 72
resend last Fax report 74
reset option 71
status and statistics option 71
voice access using 67
voice pager configuration parameters 69
voice pager messages 70
voice pager support 69
Voice/Data/Fax Modem support 67
voice pager configuration parameters of the Voice/Data/Fax Modem 69
voice pager messages 70

voice pager support using the Voice/Data/Fax Modem 69

W

Web browser interface 50, 59
bridging option 65
configuration 62
configuration and console menu 61
console monitoring 62
devices option 64
event logging system monitoring 62
guided configuration 63
IP option 65
IPX option 66
LAN emulation option 64
quick configuration 63
rules for using 59
setup 59
structure of the Home Page 60
work
LAN Emulation Services monitoring commands 403
work with ELAN
Selected SuperELAN configuration command 293
Selected SuperELAN monitoring command 304
Work with ELAN
Work with SuperELAN monitoring command 299
Work with SuperELAN
SE Services monitoring command 297
work with SuperELAN
SE Services monitoring command 298
SuperELAN configuration command 287
Work with SuperELAN monitoring command
Broadcast Manager 298
Clear counters 298
Create 298
Disable 298
Display counters 298
ELANs 298
Enable 298
Exit 299
Flush 298
List 298
Restart 298
work with SuperELAN monitoring command
Selected SuperELAN monitoring commands 298
Work with SuperELAN monitoring command
Set 299
Show cache 299
Trace 299
VLANs 299
Work with ELAN 299
world wide web interface 59
wrap
ATM monitoring commands 280
write
CONFIG command 112
LECS database sync monitoring command 445

Readers' Comments — We'd Like to Hear from You

Nways Multiprotocol Switched Services Server
Interface Configuration and
Software User's Guide

Publication No. SC30-3818-04

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____ Address _____

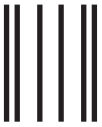
Company or Organization _____

Phone No. _____

Readers' Comments — We'd Like to Hear from You
SC30-3818-04

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Design & Information Development
Department CGF/Bldg. 656
PO Box 12195
Research Triangle Park, NC 27709-9990

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SC30-3818-04

Spine information:

Nways Multiprotocol Switched Services Server

MSS Interface Configuration