Access Server Software

Commands Reference Guide

NBase-Xyplex
295 Foster Street
Littleton, MA 01460

1-800-435-7997 (U.S.)
+978-264-9903 (International)
E-mail: support@xyplex.com
Website: www.xyplex.com

420-0559E

Warranty Information

NBase-Xyplex provides warranties for its products and services. Details of the warranty terms and conditions can be found on the following documents: Customer Product Quote Form, Order Form, Order Acknowledgment, the NBase-Xyplex price list, and on the NBase-Xyplex web site at www.xyplex.com.

NBase-Xyplex offers a variety of support contracts, including contracts that provide on-site service, telephone support, media and documentation update services, and warranty extensions. For more information on support contracts, contact your local NBase-Xyplex Sales Representative.

If you should have any questions or require assistance, please feel free to contact your local NBase-Xyplex Sales Representative or Distributor, or call NBase-Xyplex at:

In the United States:	(800) 338-5316
In Europe:	+44 81 759-1633
In Asia:	+65 336-0431

Contents

ABOUT THIS MANUAL....17
How this Manual is Organized....17
Conventions....17
ABOUT THE COMMAND LINE INTERFACE....19
USING ACCESS SERVER COMMANDS....20
Common Variables....21
Common Internet Variables....21
Reserved Keywords....23
UNIX Aliases....24
Privilege Levels....24
BACKWARDS....25
BROADCAST....26
CHECK PARAMETER SERVER....28
CLEAR/PURGE COMMANDS....29
Valid CLEAR/PURGE Commands....29
CLEAR/PURGE DOMAIN....32
CLEAR IP SECURITY....34
CLEAR PARAMETER SERVER....35
CLEAR PORT IP SECURITY....36
CLEAR/PURGE PORT IPX RIP EXPORT....37
CLEAR/PURGE PORT IPX RIP IMPORT....38
CLEAR/PURGE PORT IPX SAP EXPORT NETWORK....39
CLEAR/PURGE PORT IPX SAP IMPORT NETWORK....41
CLEAR/PURGE SERVER LPD QUEUE....43
CLEAR SERVER CCL NAME....44
CLEAR SERVER IP ROTARY....45
CLEAR SERVER IP ROUTE....46
CLEAR SERVER IP TRANSLATION TABLE....47
CLEAR/PURGE SERVER IPX RIP EXPORT....49
CLEAR/PURGE SERVER IPX RIP IMPORT....50
CLEAR/PURGE SERVER IPX SAP EXPORT NETWORK....51
CLEAR/PURGE SERVER IPX SAP EXPORT TYPE....52
CLEAR/PURGE SERVER IPX SAP IMPORT NETWORK....53
CLEAR/PURGE SERVER IPX SAP IMPORT TYPE....54
CLEAR SERVER MENU....55
CLEAR SERVER SCRIPT SERVER....56
CLEAR SERVICES....57
CLEAR XPRINTER PORTS....58
CLEAR XPRINTER....59
CONNECT....60
CONNECT PORT....63
CRASH....66
DEFINE AND SET COMMANDS....67
DEFINE/SET DOMAIN COMMANDS....68
DEFINE/SET PORT - GENERAL INFORMATION....70
Valid DEFINE/SET PORT Commands....71
DEFINE/SET PORT ACCESS....82
DEFINE/SET PORT ALTERNATE SPEED PRIVILEGE:....83
DEFINE PORT APD....84
DEFINE/SET PORT APD AUTHENTICATION....85
DEFINE/SET PORT APD DEFAULT....86

DEFINE PORT APD PROMPT 87
DEFINE PORT ARAP 89
DEFINE PORT ARAP GUEST LOGINS ENABLED/DISABLED 91
DEFINE PORT ARAP MAXIMUM CONNECT TIME 92
SET PORT ARAP TIME REMAINING 93
DEFINE PORT ARAP ZONE ACCESS 94
DEFINE/SET PORT AUTHORIZED GROUPS 95
DEFINE/SET PORT AUTOBAUD 96
DEFINE/SET PORT AUTOCONNECT 97
DEFINE/SET PORT AUTODEDICATED 98
DEFINE/SET PORT AUTOHANGUP 99
DEFINE/SET PORT AUTOPROMPT 100
DEFINE/SET PORT BACKWARD SWITCH 101
DEFINE/SET PORT BREAK 102
DEFINE/SET PORT BREAK LENGTH 103
DEFINE/SET PORT BROADCAST 104
DEFINE/SET PORT CCL MODEM AUDIBLE/INAUDIBLE 105
DEFINE PORT CCL NAME 106
DEFINE/SET PORT CHARACTER SIZE 108
DEFINE/SET PORT CLEAR IP SECURITY ENTRIES 109
DEFINE PORT COMMAND SIZE 110
DEFINE/SET PORT CONNECTRESUME 111
DEFINE/SET PORT CONTROLLED PORT 112
DEFINE/SET PORT CONTROLLED SESSION 113
DEFINE/SET PORT DCD TIMEOUT 114
DEFINE PORT DEDICATED SERVICE 115
DEFINE/SET PORT DEFAULT SESSION MODE 117
DEFINE/SET PORT DIALBACK 119
DEFINE/SET PORT DIALBACK TIMEOUT 120
DEFINE/SET PORT DIALOUT ACTION 121
DEFINE/SET PORT DIALUP 122
DEFINE/SET PORT DISCARD ERRORS 123
DEFINE/SET PORT DSRLOGOUT 124
DEFINE/SET PORT DSRWAIT 125
DEFINE/SET PORT DTRWAIT 126
DEFINE/SET PORT FLOW CONTROL 127
DEFINE/SET PORT FORWARD SWITCH 128
DEFINE PORT FROM PORT 129
SET PORT GROUPS 130
DEFINE/SET PORT IDLE TIMEOUT 132
DEFINE/SET PORT INACTIVITY LOGOUT 133
DEFINE/SET PORT INPUT FLOW CONTROL 134
DEFINE/SET PORT IP CONNECTIONS 135
DEFINE/SET PORT IP CSLIP 136
DEFINE/SET PORT IP SECURITY 138
DEFINE/SET PORT IP SLIP 140
DEFINE/SET PORT IP SLIP AUTOSEND 142
DEFINE/SET PORT IP TCP KEEPALIVE TIMER 143
DEFINE PORT IP TCP OUTBOUND ADDRESS 144
DEFINE/SET PORT IP TCP WINDOW SIZE 145
DEFINE/SET PORT INTERRUPTS 146
DEFINE/SET PORT IP FILTER 147
  Enabling IP Filtering 147
DEFINE/SET PORT IP FILTER PROTOCOL 149
DEFINE/SET PORT IP FILTER DESTINATION PORT 150

DEFINE/SET PORT IP FILTER SYN 151
DEFINE/SET PORT IP FILTER SOURCE PORT 152
DEFINE/SET PORT IP FILTER DESTINATION 153
DEFINE/SET PORT [PPP] IPX 154
DEFINE PORT IPX RIP IMPORT 157
DEFINE/SET PORT IPX RIP BROADCAST 158
DEFINE/SET PORT IPX RIP [BROADCAST] DISCARD TIMEOUT 159
DEFINE/SET PORT IPX RIP BROADCAST TIMER 160
DEFINE/SET PORT IPX RIP EXPORT NETWORK 161
DEFINE/SET PORT IPX SAP EXPORT NETWORK 162
DEFINE/SET PORT IPX SAP EXPORT TYPE 163
DEFINE/SET PORT IPX SAP IMPORT NETWORK 164
DEFINE/SET PORT IPX SAP IMPORT TYPE 165
DEFINE PORT KERBEROS 166
DEFINE/SET PORT KEYMAP 167
DEFINE PORT LAT DEDICATED SERVICE 168
DEFINE/SET PORT LAT PREFERRED SERVICE 169
DEFINE/SET PORT LIMITED VIEW 170
DEFINE/SET PORT LINE EDITOR 171
DEFINE/SET PORT LOCAL SWITCH 174
DEFINE/SET PORT LOGIN DURATION 175
DEFINE/SET PORT LOSS NOTIFICATION 176
DEFINE/SET PORT MENU 177
DEFINE/SET PORT MESSAGE CODES 178
DEFINE/SET PORT MODEM CONTROL 179
DEFINE/SET PORT MULTISESSIONS 180
DEFINE/SET PORT NAME 181
DEFINE/SET PORT NESTED MENU 182
DEFINE/SET PORT NESTED MENU TOP LEVEL 183
DEFINE/SET PORT NOLOSS 184
DEFINE/SET PORT OUTBOUNDSECURITY 185
DEFINE/SET PORT OUTPUT FLOW CONTROL 186
DEFINE/SET PORT PARITY 187
DEFINE PORT PASSWORD 188
DEFINE/SET PORT PASSWORD PROMPT 189
DEFINE/SET PORT PAUSE 190
DEFINE/SET PORT PPP 191
DEFINE/SET PORT PPP ACTIVE 192
DEFINE/SET PORT PPP CHAP CHALLENGE TIMER 193
DEFINE/SET PORT PPP CHAP RADIUS 194
DEFINE/SET PORT PPP CHARMAP 195
DEFINE/SET PORT PPP CONFIGURE LIMIT 198
DEFINE/SET PORT PPP DEFAULTS 199
DEFINE/SET PORT PPP FAILURE LIMIT 200
DEFINE/SET PORT PPP IP BROADCASTS 201
DEFINE/SET PORT PPP IP LOCAL ADDRESS 202
DEFINE/SET PORT PPP IP LOCAL ADDRESS RANGE 203
DEFINE/SET PORT PPP IP MASK 204
DEFINE/SET PORT PPP IP REMOTE ADDRESS 205
DEFINE/SET PORT PPP IP REMOTE ADDRESS RANGE 206
DEFINE/SET PORT PPP IP VJ COMPRESSION 207
DEFINE/SET PORT PPP IP VJ COMPRESSION SLOTS 208
DEFINE/SET PORT PPP IPX SAP [BROADCAST] 210
DEFINE/SET PORT [PPP] IPX SAP [BROADCAST] DISCARD TIMEOUT 211
DEFINE/SET PORT [PPP] IPX SAP [BROADCAST] TIMER 212

DEFINE/SET PORT PPP KEEPALIVE TIMER 213
DEFINE/SET PORT PPP KEEPALIVE TIMEOUT 214
DEFINE/SET PORT PPP LOGGING 215
DEFINE/SET PORT PPP MAGIC NUMBER 217
DEFINE/SET PORT PPP PAP 218
DEFINE/SET PORT PPP RESTART TIMER 220
DEFINE/SET PORT PREFERRED SERVICE 221
DEFINE/SET PORT PRIVILEGED MENU 223
DEFINE/SET PORT PRIVILEGED NESTED MENU 224
DEFINE/SET PORT PROMPT 225
DEFINE/SET PORT QUEUING 226
DEFINE/SET PORT RADIUS 227
DEFINE/SET PORT RADIUS ACCOUNTING 228
DEFINE/SET PORT RADIUS SOLICITS 229
DEFINE/SET PORT REMOTE DISCONNECT NOTIFICATION 230
DEFINE/SET PORT REMOTE MODIFICATION 231
DEFINE/SET PORT RESOLVE SERVICES 232
DEFINE/SET PORT RLOGIN DEDICATED SERVICE 233
DEFINE/SET PORT RLOGIN PREFERRED SERVICE 234
DEFINE/SET PORT RLOGIN TRANSPARENT MODE 235
SET PORT SCRIPT 236
DEFINE/SET PORT SCRIPT ECHO 237
DEFINE PORT SCRIPT LOGIN 238
DEFINE PORT SECURID 239
DEFINE/SET PORT SECURITY 240
SET PORT SESSION MODE 241
DEFINE/SET PORT SESSION LIMIT 242
DEFINE/SET PORT SIGNAL CHECK 243
DEFINE/SET PORT SLIP IP MASK 244
DEFINE/SET PORT SPEED 245
DEFINE/SET PORT STOP BITS 246
DEFINE/SET PORT TELNET ABORT OUTPUT 247
DEFINE/SET PORT TELNET ATTENTION 248
DEFINE/SET PORT TELNET BINARY SESSION MODE 249
DEFINE PORT TELNET COMPORTCONTROL 250
DEFINE/SET PORT TELNET CSI ESCAPE 254
DEFINE PORT TELNET DEDICATED SERVICE 255
DEFINE PORT TELNET DEDICATED SERVICE KICKSTART 257
DEFINE PORT TELNET DEDICATED SERVICE USERDATA 259
DEFINE/SET PORT TELNET DEFAULT 262
DEFINE/SET PORT TELNET DEFAULT TERMINALS 263
DEFINE/SET PORT TELNET ECHO MODE 264
DEFINE/SET PORT TELNET EOR REFLECTION 265
DEFINE/SET PORT TELNET ERASE CHARACTER 266
DEFINE/SET PORT TELNET ERASE LINE 267
DEFINE/SET PORT TELNET INTERRUPT 268
DEFINE/SET PORT TELNET INTERRUPTS AS BREAK 269
DEFINE/SET PORT TELNET DEFAULT LOCATION 270
DEFINE/SET PORT TELNET NEWLINE 271
DEFINE/SET PORT TELNET NEWLINE FILTERING 272
DEFINE/SET PORT TELNET OPTION DISPLAY 273
DEFINE/SET PORT TELNET PASS8D 274
DEFINE/SET PORT TELNET PREFERRED SERVICE 275
DEFINE/SET PORT TELNET QUERY 276
DEFINE/SET PORT TELNET REMOTE 277

DEFINE/SET PORT TELNET RS491 278
DEFINE/SET PORT TELNET SYNCHRONIZE 279
DEFINE/SET PORT TELNET TERMINALTYPE 280
DEFINE/SET PORT TELNET TN3270 DEFAULT 282
DEFINE/SET PORT TELNET TN3270 DEVICE 283
DEFINE/SET PORT TELNET TN3270 EOR 284
DEFINE/SET PORT TELNET TN3270 ERRORLOCK 285
DEFINE/SET PORT TELNET TN3270 PREFIXKEYMAP 286
DEFINE/SET PORT TELNET TN3270 PRINTER PORT 287
DEFINE PORT TELNET TN3270 SCANNER 288
DEFINE PORT TELNET TN3270 SPACE_INSERT 289
DEFINE/SET PORT TELNET TN3270 TRANSLATIONTABLE 290
DEFINE PORT TELNET TN3270 TYPE_AHEAD 291
DEFINE/SET PORT TELNET TN3270 XTDATTRS 292
DEFINE/SET PORT TELNET TRANSMIT 293
DEFINE/SET PORT TELNET URGENT BREAK 295
DEFINE PORT TO DEFAULTS 296
DEFINE/SET PORT TYPE 297
DEFINE/SET PORT TYPEAHEAD SIZE 298
DEFINE PORT ULI 299
DEFINE/SET PORT USER KERBEROS PASSWORD 300
DEFINE/SET PORT USERNAME FILTERING 301
DEFINE/SET PORT USERNAME PROMPT 302
DEFINE/SET PORT VERIFICATION 303
DEFINE PORT WELCOME BEFORE AUTHENTICATION 304
DEFINE PORT XDM HOST 305
DEFINE/SET PORT XDM QUERY 306
DEFINE PORT XON SEND TIMER 307
DEFINE PORT XREMOTE 308
DEFINE/SET SERVER - GENERAL INFORMATION 309
Valid DEFINE/SET SERVER Commands 310
DEFINE SERVER ACCOUNTING ENTRIES 317
DEFINE/SET SERVER ANNOUNCEMENTS 318
DEFINE SERVER APD ENABLED/DISABLED 319
DEFINE/SET SERVER APD MESSAGE 320
DEFINE SERVER ARAP DEFAULT ZONE 321
DEFINE/SET SERVER ARAP PASSWORD 322
DEFINE/SET SERVER ARAP NODE NAME 323
DEFINE/SET SERVER BROADCAST 324
SET SERVER CARDCOPY 325
SET SERVER CARDCOPY ERASE 326
DEFINE/SET SERVER CHANGE 327
SET SERVER CHASSIS 328
DEFINE/SET SERVER CIRCUIT TIMER 329
DEFINE/SET SERVER CONSOLE LOGOUT 330
DEFINE SERVER CONTROLLED PORTS 331
DEFINE SERVER CONTROLLED TERMINALS 332
DEFINE SERVER DAEMON FINGERD 333
DEFINE SERVER DAEMON LPD 334
DEFINE SERVER DAEMON ROUTED 335
DEFINE SERVER DAEMON RWHOD 336
DEFINE SERVER DAEMON SYSLOGD 337
SET SERVER DATE 339
DEFINE/SET SERVER DUMP 340
DEFINE SERVER DUMP PROTOCOL 341

DEFINE/SET SERVER EVENTLOG 343
SET SERVER FORMAT CARD 344
SET SERVER GET CARD 345
DEFINE/SET SERVER HEARTBEAT 346
DEFINE SERVER HELP 347
DEFINE/SET SERVER IDENTIFICATION 348
DEFINE/SET SERVER IDENTIFICATION SIZE 349
DEFINE SERVER IMAGE [LOAD] PROTOCOL 350
DEFINE/SET SERVER INACTIVITY TIMER 351
DEFINE/SET SERVER INTERNET OR IP COMMANDS 352
DEFINE/SET SERVER IP ADDRESS 353
DEFINE SERVER IP ADDRESS AUTODISCOVERY 354
DEFINE/SET SERVER IP BROADCAST ADDRESS 356
DEFINE/SET SERVER IP DEFAULT DOMAIN SUFFIX 357
DEFINE/SET SERVER IP DOMAIN ADDRESS 359
DEFINE SERVER IP HOST 360
DEFINE SERVER INTERNET IP REASSEMBLY 361
DEFINE/SET SERVER IP LOAD FILE 362
DEFINE/SET SERVER INTERNET NAME 363
DEFINE/SET SERVER IP DELIMITER 364
DEFINE/SET SERVER IP DOMAIN TTL 365
DEFINE/SET SERVER IP FILTER 366
DEFINE/SET SERVER IP FILTER DESTINATION 367
DEFINE/SET SERVER IP FILTERING 368
DEFINE/SET SERVER IP FILTER PROTOCOL 369
DEFINE/SET SERVER IP FILTER SOURCE 370
DEFINE/SET SERVER IP FILTER SYN 371
DEFINE/SET SERVER IP GATEWAY ADDRESS 372
DEFINE/SET SERVER IP GATEWAY TIMEOUT 373
DEFINE/SET SERVER IP NAME 374
DEFINE/SET SERVER IP LOCAL BASE 375
DEFINE/SET SERVER IP ROTARY 376
DEFINE/SET SERVER IP ROUTE 377
DEFINE SERVER IP ROUTING TABLE SIZE 380
DEFINE SERVER IP SECURITY 381
DEFINE/SET SERVER IP SNMP AUTHENTICATION TRAPS 382
DEFINE/SET SERVER IP SNMP CLIENT 383
DEFINE/SET SERVER IP SNMP COMMUNITY 385
DEFINE/SET SERVER IP SNMP SYSTEM CONTACT/LOCATION 387
DEFINE/SET SERVER IP SUBNET MASK 388
DEFINE/SET SERVER IP SUBNET MASK AUTOCONFIGURE 389
DEFINE/SET SERVER IP TCP CONNECT TIMER 390
DEFINE SERVER IP TCP RESEQUENCING 391
DEFINE/SET SERVER IP TCP RETRANSMIT 392
DEFINE/SET SERVER IP TRANSLATION TABLE TTL 393
DEFINE/SET SERVER IP TTL 394
DEFINE/SET SERVER IPX FILTER DESTINATION NETWORK 395
DEFINE/SET SERVER IPX FILTER DESTINATION NODE 396
DEFINE/SET SERVER IPX FILTER DESTINATION SOURCE 397
DEFINE/SET SERVER IPX FILTER PACKET 398
DEFINE/SET SERVER IPX FILTER SOURCE NETWORK 399
DEFINE/SET SERVER IPX FILTER SOURCE NODE 400
DEFINE SERVER IPX FILTERING 401
DEFINE SERVER IPX INTERNAL NETWORK 402
DEFINE SERVER IPX NETWORK 403

DEFINE SERVER IPX PROTOCOL 404
DEFINE/SET SERVER IPX RIP BROADCAST 405
DEFINE/SET SERVER IPX RIP BROADCAST DISCARD TIMEOUT 406
DEFINE/SET SERVER IPX RIP BROADCAST TIMER 407
DEFINE/SET SERVER IPX RIP EXPORT 408
DEFINE SERVER IPX RIP IMPORT NETWORK 409
DEFINE SERVER IPX RIP MAXIMUM TABLE SIZE 410
DEFINE/SET SERVER IPX SAP BROADCAST 411
DEFINE/SET SERVER IPX SAP BROADCAST DISCARD TIMEOUT 412
DEFINE/SET SERVER IPX SAP BROADCAST TIMER 413
DEFINE/SET SERVER IPX SAP EXPORT NETWORK 414
DEFINE/SET SERVER IPX SAP EXPORT TYPE 415
DEFINE/SET SERVER IPX SAP IMPORT NETWORK 416
DEFINE/SET SERVER IPX SAP IMPORT TYPE 417
DEFINE SERVER IPX SAP MAXIMUM TABLE SIZE 418
DEFINE/SET SERVER KEEPALIVE TIMER 419
DEFINE SERVER KERBEROS 420
DEFINE/SET SERVER KERBEROS ERROR MESSAGE 421
DEFINE SERVER KERBEROS FIVE 422
DEFINE/SET SERVER KERBEROS MASTER 423
DEFINE/SET SERVER KERBEROS PASSWORD PORT 424
DEFINE/SET SERVER KERBEROS PASSWORD SERVICE 425
DEFINE/SET SERVER KERBEROS PORT 426
DEFINE/SET SERVER KERBEROS PRIMARY/SECONDARY SERVER....427
DEFINE/SET SERVER KERBEROS QUERY LIMIT 428
DEFINE/SET SERVER KERBEROS REALM 429
DEFINE/SET SERVER KERBEROS SECURITY 430
DEFINE/SET SERVER LAT IMMEDIATE ACK 431
DEFINE/SET SERVER LAT SOLICITS 432
DEFINE SERVER LOAD IP ADDRESS 433
DEFINE/SET SERVER LOAD IP DELIMITER 434
DEFINE SERVER LOAD IP LOAD FILE 435
DEFINE SERVER LOAD IP GATEWAY 436
DEFINE SERVER LOAD IP LOAD HOST 437
DEFINE SERVER LOAD PROTOCOL 438
DEFINE SERVER LOAD SOFTWARE 440
DEFINE SERVER LOADDUMP 441
DEFINE SERVER LOADDUMP DEFAULT 442
DEFINE SERVER LOAD STATUS MESSAGE 443
DEFINE/SET SERVER LOCK 444
DEFINE/SET SERVER LOGIN PASSWORD 445
DEFINE/SET SERVER LOGIN PROMPT 446
DEFINE/SET SERVER LPD QUEUE 447
DEFINE/SET SERVER LPD QUEUE BYPASS 450
DEFINE/SET SERVER MAINTENANCE PASSWORD 451
DEFINE SERVER MENU 452
DEFINE/SET SERVER MENU CONTINUE PROMPT 453
DEFINE/SET SERVER MENU PROMPT 454
DEFINE/SET SERVER MULTICAST TIMER 455
DEFINE SERVER MULTISESSIONS 456
DEFINE/SET SERVER NAME 457
DEFINE SERVER NESTED MENU NAME 458
DEFINE SERVER NESTED MENU SIZE 459
DEFINE/SET SERVER NODE LIMIT 460
DEFINE/SET SERVER NUMBER 461

DEFINE SERVER OVERRIDE INTERNAL ADDRESS 462
DEFINE SERVER PACKET COUNT 463
DEFINE/SET SERVER PARAMETER SERVER CHECK 464
DEFINE/SET SERVER PARAMETER SERVER PATH 466
DEFINE/SET SERVER PARAMETER SERVER LIMIT 467
DEFINE/SET SERVER PARAMETER SERVER RETRANSMIT 468
DEFINE/SET SERVER PASSWORD LIMIT 469
DEFINE/SET SERVER PAP REMOTE PASSWORD 470
DEFINE SERVER PPP CHAP REMOTE PASSWORD 471
DEFINE/SET SERVER PRIVILEGED PASSWORD 472
DEFINE SERVER PROTOCOL ARAP 473
DEFINE SERVER PROTOCOL IPX 474
DEFINE SERVER PROTOCOL LAT 475
DEFINE SERVER PROTOCOL MX800 476
DEFINE SERVER PROTOCOL PPP 477
DEFINE SERVER PROTOCOL SNMP 478
DEFINE SERVER PROTOCOL TELNET 479
DEFINE SERVER PROTOCOL TN3270 480
DEFINE SERVER PROTOCOL XPRINTER 481
DEFINE SERVER PROTOCOL XREMOTE 482
DEFINE/SET SERVER PURGE GROUP 483
DEFINE/SET SERVER PURGE NODE 484
DEFINE/SET SERVER QUEUE LIMIT 485
DEFINE SERVER RADIUS 486
DEFINE/SET SERVER RADIUS ACCOUNTING 487
DEFINE/SET SERVER RADIUS CHAP CHALLENGE SIZE 488
DEFINE/SET SERVER RADIUS LOGGING 489
DEFINE/SET SERVER RADIUS PORT 490
DEFINE/SET SERVER RADIUS PRIMARY/SECONDARY SECRET 491
DEFINE/SET SERVER RADIUS PRIMARY/SECONDARY SERVER 492
DEFINE/SET SERVER RADIUS SERVER RETRY 493
DEFINE/SET SERVER RADIUS TIMEOUT 494
DEFINE/SET SERVER RELIABLE ACCOUNTING 495
DEFINE/SET SERVER REPORT ERRORS 496
DEFINE/SET SERVER RETRANSMIT LIMIT 497
DEFINE/SET SERVER SOFTWARE 498
DEFINE SERVER RIP STATE 499
DEFINE/SET SERVER RLOGIN 500
DEFINE SERVER ROTARY ROUNDROBIN 501
DEFINE/SET SERVER SCRIPT SERVER 502
DEFINE SERVER SECURID ENABLED/DISABLED 503
DEFINE SERVER SECURID ACMBASETIMEOUT 504
DEFINE/SET SERVER SECURID ACMMAXRETRIES 505
DEFINE/SET SERVER SECURID ACM_PORT 506
DEFINE/SET SERVER SECURID ENCRYPTION MODE 507
DEFINE/SET SERVER SECURID QUERY LIMIT 508
DEFINE/SET SERVER SECURID SERVER*N* 509
DEFINE/SET SERVER GROUPS 510
DEFINE/SET SERVER SERVICES GROUPS 511
DEFINE SERVER SESSION LIMIT 512
DEFINE/SET SERVER TCP ACK DELAYED 513
DEFINE/SET SERVER TEXTPOOL SIZE 514
DEFINE/SET SERVER TIME SERVER 515
DEFINE/SET SERVER TIMEZONE 516
DEFINE SERVER TN3270 DEVICE 517

DEFINE SERVER TN3270 DEVICE SCREENMAP COLOR 523
DEFINE SERVER TN3270 DEVICE KEYMAP NUM_OVERRIDE 524
DEFINE SERVER TN3270 DEVICE NAME 525
DEFINE SERVER TN3270 TRANSLATIONTABLE 527
DEFINE SERVER ULI 528
DEFINE SERVER USE DEFAULT PARAMETERS 529
DEFINE/SET SERVER USERDATA DELAY 530
DEFINE/SET SERVER VERBOSE ACCOUNTING 531
DEFINE/SET SERVER VERBOSE PRIORITY 532
DEFINE/SET SERVER WELCOME 534
DEFINE/SET XPRINTER 535
DEFINE SERVER XPRINTER DATA TIMEOUT 536
DEFINE/SET SERVER XREMOTE FONT SERVER 537
SET SERVER PARAMETER VERSION 538
DEFINE/SET SERVICE 539
DEFINE/SET PARAMETER SERVER 542
DISCONNECT 543
FORWARDS 544
GET CARD LOAD FILE 546
GET CARD STOP 547
HELP 548
INITIALIZE SERVER 549
LAT CONNECT 551
LAT CONNECT PORT 553
LIST 554
LOCK 555
LOGOUT PORT 556
MONITOR 557
PURGE DOMAIN 558
PURGE MANAGER 559
PURGE SERVER IP ROTARY 561
PURGE [PORT] IP SECURITY 562
PURGE PARAMETER SERVER 563
PURGE PORT IP SECURITY 564
PURGE SERVER IP ROUTE 565
PURGE SERVER MENU 566
PURGE SERVER SCRIPT SERVER 567
PURGE SERVER TN3270 DEVICE 568
PURGE SERVER TN3270 TRANSLATIONTABLE 569
PURGE SERVICES 570
PURGE XPRINTER PORTS 571
REFRESH SERVER CCL NAME 572
REMOTE CONSOLE 574
REMOVE QUEUE 577
RESET PORT 578
RESUME 579
RLOGIN 581
SCRIPT 583
SET - GENERAL INFORMATION 584
SET DOMAIN 585
SET PORT 586
SET SERVER 587
SET SERVER CHASSIS 588
SET SERVER COPY 589
SET SERVER TIME 590

SET SERVICE 591
SET NOPRIVILEGED 592
SET PARAMETER SERVER 593
SET PRIVILEGED/NOPRIVILEGED 594
SET SESSION 596
SHOW/LIST/MONITOR - GENERAL INFORMATION 598
Valid Show, List and Monitor Commands: 600
SHOW/MONITOR CARD STATUS 601
SHOW/LIST/MONITOR CHASSIS 603
SHOW/MONITOR DESTINATIONS 604
SHOW/MONITOR/LIST DOMAIN 605
SHOW/LIST/MONITOR PORT LINE EDITOR CHAR 607
SHOW/LIST/MONITOR MANAGER 609
SHOW/MONITOR NODES 612
SHOW/LIST/MONITOR PARAMETER SERVER 618
SHOW/LIST/MONITOR PORT ACCESS 623
SHOW/LIST/MONITOR PORT ALT CHARACTERISTICS 626
SHOW/LIST/MONITOR PORT ARAP CHARACTERISTICS 632
SHOW/MONITOR PORT ARAP COUNTERS 634
SHOW/LIST/MONITOR PORT CHARACTERISTICS 636
SHOW/MONITOR/LIST PORT CONTROLLED 645
SHOW/MONITOR PORT COUNTERS 646
SHOW/LIST/MONITOR PORT IP SECURITY 650
SHOW/LIST/MONITOR PORT KEYMAP 652
SHOW/LIST/MONITOR PORT PPP CHARACTERISTICS 654
SHOW/MONITOR PORT PPP COUNTERS 657
SHOW/MONITOR PORT PPP IP CHARACTERISTICS 659
SHOW/MONITOR PORT PPP IP COUNTERS 661
SHOW/MONITOR PORT PPP IP STATUS 662
SHOW/MONITOR PORT PPP STATUS 663
SHOW/LIST PORT SCREENMAP 664
SHOW/MONITOR PORT STATUS 665
SHOW/LIST/MONITOR PORT SUMMARY 672
SHOW/LIST/MONITOR PORT TELNET CHAR 677
SHOW/LIST PORT TELNET COMPORTCONTROL CHAR 682
SHOW/LIST/MONITOR SERVER - GENERAL INFORMATION 685
SHOW/MONITOR SERVER ACCOUNTING 686
SHOW/MONITOR SERVER ALTERNATE STATUS 690
SHOW/LIST SERVER ARAP CHARACTERISTICS 693
SHOW SERVER CCL 694
SHOW/LIST/MONITOR SERVER CHARACTERISTICS 695
SHOW/MONITOR SERVER COUNTERS 699
SHOW/LIST/MONITOR SERVER IP CHARACTERISTICS 703
SHOW/MONITOR SERVER IP COUNTERS 706
SHOW/LIST/MONITOR SERVER IP ICMP COUNTER 710
SHOW/LIST/MONITOR SERVER IP ROTARY 713
SHOW/LIST/MONITOR SERVER IP ROUTES 714
SHOW/LIST/MONITOR SERVER IP SECURITY 716
SHOW/LIST/MONITOR SERVER IP SNMP CHAR 718
SHOW/MONITOR SERVER IP SNMP COUNTERS 720
SHOW/MONITOR SERVER IP TRANSLATION TABLE 723
SHOW/LIST/MONITOR SERVER KERBEROS 725
LIST/MONITOR SERVER LOADDUMP CHARACTERISTICS 731
SHOW/MONITOR SERVER LPD COUNTERS 733
SHOW/LIST/MONITOR SERVER LPD QUEUE 735

SHOW/MONITOR SERVER LPD STATUS 738
SHOW/LIST/MONITOR SERVER MENU 739
SHOW/LIST/MONITOR SERVER RADIUS 740
SHOW/LIST/MONITOR SERVER SCRIPT SERVER 742
SHOW/LIST/MONITOR SERVER SECURID 743
SHOW/MONITOR SERVER STATUS 746
SHOW/LIST/MONITOR SERVER SUMMARY 750
SHOW/LIST SERVER TN3270 751
SHOW/LIST SERVER TN3270 DEVICE 752
SHOW/LIST SERVER TN3270 TRANSLATIONTABLE 755
SHOW/LIST/MONITOR SERVER XREMOTE 757
SHOW/LIST/MONITOR SERVICES CHARACTERISTICS 759
SHOW/MONITOR SERVICES STATUS 762
SHOW/MONITOR SERVICES SUMMARY 765
SHOW/MONITOR SESSIONS 767
SHOW UNIT 771
SHOW/MONITOR USER STATUS 773
SHOW/MONITOR USERS 774
SHOW XPRINTER 778
SHOW/LIST XPRINTER PORTS 779
TELNET CONNECT 780
TELNET CONNECT PORT 782
TELNET CONSOLE 784
TEST IP 786
TEST LOOP 787
TEST PORT 788
TEST SERVICE 789
ULI 791
XCONNECT 792
ZERO COUNTERS 793

About this Manual

This manual provides a command reference for the NBase-Xyplex Access Server software. It describes the name, description, notes, privilege level, syntax, and other information about each access server command.

How this Manual is Organized

This manual is organized as follows:

Topic	Describes
Introduction	Provides a brief introducing to the command line interface, describes how to use access server commands, and describes command options, keywords, and variables. It also discusses UNIX aliases.
Command Reference	Presents, in alphabetical order, a detailed description of all the access server commands.

Conventions

The *Commands Reference Guide* uses the following conventions

Convention	Explanation
RETURN	Unless otherwise specified, commands execute when you press the RETURN key on the keyboard. This manual assumes that you press RETURN after typing each command line and does not note the use of the RETURN key.
CTRL CTRL/X	The CONTROL (CTRL) key on the keyboard provides alternate functions when used with some keyboard keys. CTRL/T indicates that you press both the CTRL key and the letter T key at same time. This is echoed on your screen as ^T.
COMMAND	Access server commands appear in uppercase letters. However, the commands are not case sensitive except where noted. Although you can abbreviate most commands, commands appear fully spelled out in this manual.
KEYWORD	Keywords appear in uppercase letters. Keywords identify the action you are performing, or the type of object on which the action is performed. When you enter a command, you must type each keyword (or keyword abbreviation) exactly as it appears in the syntax description.
variable	Variables appear in the text as lowercase italics. Variables identify information that you must supply in a command line, such as the port number. A variable can be a single character, a text message, a number, a CTRL command, and so on.

`monospace font`	Monospace font indicates text that can be displayed or typed at a terminal, such as displays, user input, messages, prompts, system responses, and so on.
`Xyplex>`	The access server user prompt with only a single > indicates secure and non-privileged mode. This prompt indicates that the server is waiting for a command. Note that this is the default prompt name. The server manager can specify a different prompt name, so the prompt in use at your site may differ.
`Xyplex>>`	The Xyplex access server user with a double >> indicates privileged mode. Note that this is the default prompt name. The server manager can specify a different prompt name, so the prompt in use at your site may differ.
`Xyplex> commands`	Your input at a system prompt appears after the prompt in monospace font.
`COMMAND [OPTION 1]` `[OPTION 2]`	Choices that you can enter as part of a command line, such as command options, appear inside right and left square brackets. This manual also lists by vertical alignment to denote options. Do not type the brackets.
`[[OPTION] option]`	Options can apply within options, and are indicated by nested square brackets.
`$`	This is the default system prompt for VMS.
`%`	This is the default system prompt for UNIX/ULTRIX.
`C:\`	This is the default system prompt for DOS.

About the Command Line Interface

The access server software provides a series of commands and CTRL characters that you enter at a prompt. This command line user interface (CLI) lets you perform the following tasks:

- Establish, monitor, and control server sessions
- Control communications between the server and devices (such as terminals and modems) as well as between the server and service nodes
- Control and monitor the availability of services which are offered at server ports
- Use security features of the access server software
- Recover if problems occur

For a detailed description of each command, see the command reference pages later in this guide .

The following section gives a brief summary on how to use access server commands; for a more complete discussion on using the access server user interface, see *Configuration Guide.*

Using Access Server Commands

The following list provides some notes on using the access server commands:

- To execute most commands, type the command at the local prompt (`Xyplex>`) and press RETURN. The commands are not case sensitive, so you do not have to enter them in uppercase letters. You can abbreviate commands to the shortest unambiguous string of characters.

- The maximum length of a command line is 132 characters. You can type a command that exceeds the width of the terminal screen as long as you do not press the RETURN key until the command is complete.

- For most commands, you can specify multiple keywords or variables with a single command. When you specify a single command that applies to more than one characteristic, separate the characteristics with one or more spaces, a comma, or any combination of commas and spaces.

- Commands have defined privilege levels that are noted on the command reference pages. Secure users have limited privileges, non-privileged users have more privileges, and privileged users can use all of the commands and functions. Users on privileged ports see the `Xyplex>>` prompt followed by two angle brackets instead of one for secure and non-privileged users.

- When you execute a command that affects more than one port, or that contains multiple characteristics in the same command, the software first verifies that all requested actions are valid before performing them. If any individual action would display an error message, the software performs none of the requested actions.

- CTRL commands let you edit the current command line before you press RETURN, or recall previous command lines for editing.

- You can assign session management functions to character sequences using the SET PORT command. This lets you access session management functions from within sessions, rather than entering equivalent commands from the `Xyplex>` prompt.

- Some of the DEFINE SERVER Commands require the server be initialized for the changes to take effect. Always reboot the server using the INIT DELAY command to prevent corruption of the parameter storage. Commands that require reinitialization will display the following message when the RETURN key is pressed:

  `XYPLEX - 705 - CHANGE LEAVES APPROXIMATELY XXXXXXX BYTES FREE`

  These commands cannot be modified by a SET command, because the server must redistribute memory resources for the feature during the boot-up process.

Common Variables

This table defines the common variables used in command descriptions:

Variable	Description
node name	Specifies the name of a node (such as a computer or access server) in a LAT network at which a service is offered. LAT *node names* are distinct from DECnet *node names*; however, Xyplex recommends that you set the LAT *node name* for a server to be the same as the DECnet node name. For a LAT *node name* , you can specify a name that consists of 1 to 16 ASCII characters, including the letters A through Z, the numbers 0 through 9, and the dollar sign ($), period (.), hyphen (-), and underscore (_) characters. (DECnet *node names*; are limited to 6 characters.) Lower-case letters in the *node name* are always translated by the software to upper-case letters. Do not enclose *node names* in quotation marks (").
port name	Specifies the name for a port. The port name can be between 1 and 16 ASCII characters in length. (Note that the server converts any lower-case letters to upper case.) Do not enclose the port name in quotation mark characters ("). The port name must be unique within each server. The default value for this variable is in the form: PORT_*port number*, where *port number* is the number of the physical server port.
port number	The number assigned to the port connector of the server hardware unit to which a device is attached. Valid values for a *port number* are one or two-digit numbers in the range of 0 to n, where n represents the number of physical ports that the unit contains. (For example, on a 40-port access server, the physical *port numbers* are in the range of 1 to 40.) The Remote Console port *port number* is always Port 0.
port-list	A list of one or more *port numbers*. You can specify multiple ports in a *port-list* by specifying individual *port numbers* separated by commas, by specifying a range of *port numbers* separated by a hyphen, or a combination of both (do not include spaces). For example, the *port-list*: 1,3-5,8 refers to the individual port settings: 1, 3, 4, 5, and 8.
service-name	The name of a LAT service that is available on the network. Specify a name that consists of 1 to 16 ASCII characters, including the letters A through Z, the numbers 0 through 9, and the dollar sign ($), period (.), hyphen (-), and underscore (_) characters. Lower-case letters in *service-name* are translated to upper-case letters. Do not enclose *service-names* in quotation marks (").

Common Internet Variables

The following table defines the internet variables used frequently in command descriptions:

Variable Name	Description
domain-name	This variable applies to TCP/IP communications. A *domain-name* identifies an addressable network object, such as a host or server. A *domain-name* maps to an *internet-address* (the server converts the *domain-name* to an *internet-address* when it communicates over the network). The network object represented by a *domain-name* runs internet protocols. You can think of a *domain-name* as a logical name for an *internet-address*. A fully-qualified *domain-namee*: The name can consist of up to 50 ASCII characters, including the letters A-Z (lower-case letters are treated as upper-case letters), the numbers 0-9, the underscore (_) and hyphen (-) characters. Separate each segment within a *domain-name* specification with a period. Each segment in the *domain-name* can be up to 50 ASCII characters in length. The left-most segment identifies the individual network object. The remaining segments identify the domain where the object is located. Do not enclose *domain names* in quotation marks ("). Examples: NIC.DDN.MIL or XYPLEX.COM. A fully qualified *domain-name* must contain at least one period. If you type a name in a Telnet command that does not contain at least one period, the software appends the default *domain-suffix* to obtain a fully qualified *domain-name*. (Specify the default *domain-suffix* using the DEFINE/SET SERVER IP DEFAULT DOMAIN SUFFIX command.)
internet-address	This variable applies to TCP/IP sessions. An *internet-address* identifies a network addressable object, such as a host or server. The network object runs internet protocols. An *internet-address* consists of four numbers separated by periods (.). Valid values for each of the four numbers are whole numbers in the range of 1 through 254 (the numbers 0 and 255 are permitted in some circumstances). An example of an *internet-address* is: 128.10.2.30.
telnet-port number	This variable applies to Telnet sessions. A *telnet-port number* is a protocol identifier. Valid values for the *telnet-port number* are whole numbers from 1-32767. Values between 1-255 represent "well-known" protocols. The default value is 23. A value other than 23 must represent a Telnet-compatible protocol. Always use a colon (:) to separate the *telnet-port number* from a *domain-name* or *internet-address*. You can use a *telnet-port number* as the address of a specific port on a server when in a Telnet session. Use this formula to specify the default port address: *telnet-port number* = [2000 + (100 x *n*)] where *n* is the physical port number. (For a Telnet session, you can specify the address of a physical port using the PORT TELNET REMOTE settings.)

Reserved Keywords

The following keywords are reserved; you cannot use them (or their abbreviations) to specify a LAT service name:

```
ALL                     INTERACTIVE             SERVICE
CHARACTERISTICS         LIMITED                 SIGNAL
CONNECTIONS             LOCAL                   STATUS
CR                      NODE                    SUMMARY
FILTERING               PASSWORD                TCP WINDOW
IDENTIFICATION          PORTS                   TRANSPARENT
IDENTIFICATION SIZE     QUEUE
```

Similarly, you cannot use the following keywords, or abbreviations of these keywords, to specify a *domain-name*

```
ALL                     LEARNED
CR                      LIMITED
FILTERING               LOCAL
IDENTIFICATION SIZE     SIGNAL
INTERACTIVE             TCP WINDOW
                        TRANSPARENT
```

UNIX Aliases

The access server software provides several UNIX-like commands, called UNIX aliases, that give the software more of a UNIX "look-and-feel". These aliases provide the same function as an access server command. The following list shows the access server commands and their corresponding UNIX aliases:

Xyplex Command	UNIX Alias
SHOW PORT [port-list] STATUS	STATUS [port-list]
RESUME *session-number*	FG *session-number*
HELP	MAN
SHOW SESSIONS	JOBS
SHOW USERS	WHO
TEST IP *host* [RECORDROUTE] [NORECORDROUTE]	PING *host* [RECORDROUTE] [NORECORDROUTE]
DISCONNECT [*session*]	CLOSE or KILL [*session*]
TELNET CONNECT [*domain-name*] [*IP-address*]	OPEN [*domain-name*] [*IP-address*]
LOGOUT [*port-list*]	QUIT [*port-list*]

Privilege Levels

The following table describes the codes for privilege levels:

Code	Description
S	Secure. Secure users, non-privileged users, and privileged users can use this command.
N	Non-Privileged. Non-privileged users and privileged users can use this command.
P	Privileged. Only privileged users can use this command.

***Note**: Default settings for each option appear in boldface font.*

BACKWARDS Privilege: S, P

The BACKWARDS command connects you from the current session to the next lower-numbered session.

The unit assigns a session number for each session to which a port is connected. Use the BACKWARDS command to select the next available, lower-numbered session to which your port or terminal is connected. For purposes of the BACKWARDS command, the unit tracks session numbers in a "circular" manner. Therefore, when a port is already connected to the lowest numbered session, typing BACKWARDS connects the port to the highest numbered session. When only one session is active at a port, the BACKWARDS command re-connects the port to that session.

You can use the backward switch character, if one is defined for your port, instead of the BACKWARDS command. For more information on this command, see DEFINE/SET PORT BACKWARD SWITCH command.

Syntax BACKWARDS

Example

This example shows you how to use the BACKWARDS command to connect to sessions from among three different sessions. Suppose that there are three sessions running at a port, and the SHOW SESSION display for this port appears as shown in the following display.

```
Xyplex> SHOW SESSIONS

Port 1:  J. Smith         Service Mode     Current Session 2
- Session 1: Connected    Interactive      FINANCEVAX (FINANCEVAX)
- Session 2: Connected    Interactive      UNIXVAX (UNIXVAX)
- Session 3: Connected    Interactive      LASER (LASER)
```

Sample SHOW SESSION Display

As shown, the port is connected to three sessions, numbered 1, 2 and 3. Session 2 is the currently active session. From the Xyplex> prompt, if you type:

```
Xyplex> BACKWARDS
```

the unit will connect the port to session number 1, which is the next available lower numbered session. If you return to the Xyplex> prompt and again type:

```
Xyplex> BACKWARDS
```

the unit will connect the port to session number 3.

BROADCAST Privilege: N, P

Use this command to send a message to one or more specified ports or to all ports on the local access server. A number of conditions apply to the server and the ports to which messages can be sent.

For the server, the BROADCAST command only works when SERVER BROADCAST is ENABLED. (See the DEFINE/SET SERVER BROADCAST command.)

For the port, broadcast messages can only be sent to ports that are logged on. The PORT BROADCAST setting must also be enabled. The port cannot be locked (via the access server LOCK command), connected to a dedicated service, or performing a MONITOR command. (You can use the SHOW PORT ALL command to determine if a port is available.)

Privileged users can broadcast a message to multiple ports or to all ports. Non-privileged users can broadcast a message to only one port at a time. The BROADCAST command is not available to secure users.

Syntax

```
BROADCAST PORT [port-list] [“message”]
               [ALL]
```

Where	Means
PORT	The message is to be broadcast only to the port(s) specified by the *port-list*.
port-list	The port(s) to which the message is sent.
ALL	The message is broadcast to all ports on the access server.
”message’	The text that displays at the port(s) listed in the *port-list* or all ports. The message can be any length, as long as the entire command does not exceed 132 characters. You must enclose the message in quotation marks ("). You can include a bell character (CTRL-G) in the text message.

Example

```
BROADCAST ALL "PAB's going-away party at 1830 today."
```

The user is broadcasting a message about a celebration to all users on the access server. This can only be done by a privileged access server user. The message will be displayed at all terminals exactly as it was typed. For example, the users at the receiving terminals might see the message as:

```
Xyplex -501- From port 1, Isaacs
PAB's going-away party at 1830 today.
```

BROADCAST (continued)

```
BROADCAST PORT 1 "^G Printer jammed, re-spool print job."
```

The user is broadcasting a message to a specific user or terminal. Non-privileged users can broadcast a message in this manner. The user at the receiving terminal would hear a "beep" sound and see a message such as:

```
Xyplex -501- From port 8, Mikey
   Printer jammed, re-spool print job.
```

CHECK PARAMETER SERVER Privilege: P

Use the CHECK PARAMETER SERVER command to force the server to locate additional, eligible parameter servers (i.e., nodes where access server parameters can be stored). During normal operation, the server performs this action periodically to insure that a parameter server is available from which the server can obtain parameter information. (The frequency at which this occurs is defined by the SET PARAMETER SERVER CHECK TIMER settings. The maximum number of eligible parameter servers, about which the server retains information, is specified using the SET SERVER PARAMETER SERVER LIMIT characteristic.) The CHECK PARAMETER SERVER command requires that the server perform this search immediately, rather than wait for the check timer period to elapse. Note that, the server attempts to keep up to date the parameters stored at all eligible parameter servers.

The Console LED will flash whenever there are permanent parameters that have not yet been stored by at least one parameter server.

Syntax

```
CHECK PARAMETER SERVER
```

Example

```
CHECK PARAMETER SERVER
```

CLEAR/PURGE Commands

Use the CLEAR command to delete the following entries in the operational database. Using the CLEAR command to delete entries lets you re-enable the setting using a SET command.

Use the PURGE command when you want to delete entries from the permanent database.

You can use the DEFINE command to respecify deleted *entries*. If the entry is listed in the operational database, it will still be available until the server is re-initialized or it is removed using a CLEAR command. The following table lists all clear/purge commands and their availability as either a CLEAR or PURGE COMMAND.

Command	Clear	Purge
ACCOUNTING	X (P)	—
CCL ALL	X (P)	—
CCL NAME	X (P)	—
DOMAIN <name>	X (P)	X (P)
DOMAIN ALL	X (P)	X (P)
DOMAIN ENTRY	X (P)	X (P)
DOMAIN LEARNED	X (P)	X (P)
DOMAIN LOCAL	X (P)	—
IP ROTARY	X (P)	X (P)
IP ROUTES	X (P)	X (P)
IP SECURITY	X (P)	X (P)
LPD QUEUE	X	X
MANAGER	—	X (P)
MANAGER ALL	—	X (P)
MANAGER GLOBAL TYPE	—	X (P)

Valid CLEAR/PURGE Commands (continued)

Command	Clear	Purge
MANAGER LOCAL TYPE	—	X (P)
MANAGER NODE ADDRESS	—	X (P)
MANAGER PARAMETER	—	X (P)
MENU	X (P)	X(P)
PARAMETER SERVER	X (P)	X (P)
PORT IP FILTER	X (P)	X (P)
PORT IP FILTER SECURITY	X (P)	X (P)

PORT IP FILTER DESTINATION	X (P)	X (P)
PORT IP FILTER DESTINATION PORT	X (P)	X (P)
PORT IP FILTER PROTOCOL ALL	X (P)	X (P)
PORT IP FILTER PROTOCOL TCP	X (P)	X (P)
PORT IP FILTER PROTOCOL UDP	X (P)	X (P)
PORT IP FILTER SOURCE	X (P)	X (P)
PORT IP FILTER SYN	X (P)	X (P)
RADIUS ACCOUNTING	X (P)	X (P)
RADIUS AUTHENTICATION	X (P)	X (P)
SCRIPT SERVER	X (P)	X (P)
SERVER ACCOUNTING	X (P)	—
SERVER CCL NAME	X (P)	—
SERVER IP DOMAIN	X (P)	—

Valid CLEAR/PURGE Commands (continued)

Command	Clear	Purge
SERVER IP FILTER	X (P)	—
SERVER IP FILTER DESTINATION	X (P)	—
SERVER IP ROTARY	X (P)	—
SERVER IP ROUTES	X (P)	—
SERVER IP TRANSLATION TABLE	X (P)	—
SERVER LPD QUEUE	—	—
SERVICES	X (P)	—
TERMINALS IP FILTER	X (P)	X (P)
TERMINALS IP SECURITY	X (P)	X (P)
TERMINALS IPX FILTER ALL	X (P)	X (P)
TERMINALS IPX FILTER DESTINATION NETWORK	X (P)	X (P)
TERMINALS IPX FILTER DESTINATION NODE	X (P)	X (P)
TERMINALS IPX FILTER PACKET	X (P)	X (P)
TERMINALS IPX FILTER PACKET ALL	X (P)	X (P)
TERMINALS IPX FILTER PACKET TYPE	X (P)	X (P)
TERMINALS IPX FILTER SOURCE NETWORK	X (P)	X (P)
TERMINALS IPX FILTER SOURCE NODE	X (P)	X (P)
TERMINALS IPX RIP	X (P)	X (P)
TERMINALS IPX SAP	X (P)	X (P)
XPRINTER	X (P)	X (P)
XPRINTER ALL	X (P)	X (P)
XPRINTER PORTS	X (P)	X (P)
XPRINTER TERMINALS	X (P)	X (P)

CLEAR/PURGE DOMAIN Privilege: P

Use the CLEAR DOMAIN command to delete, from the operational database, one or more *domain-name* entries known by the server. The deleted *domain-name(s)* can be re-enabled using a SET DOMAIN command or "learned" from a Domain name server. If the *domain-name* is listed in the permanent database, it will again be made available when the server is re-initialized.

If the specified *domain-name* is not a fully qualified *domain-name*, the specified name will be concatenated with the default Internet *domain-name-suffix*. The server will display an error message if you use the CLEAR DOMAIN command when the specified Domain name does not exist.

Syntax

```
CLEAR DOMAIN [DOMAIN-NAME]
             [ALL]
             [ENTRY ENTRY-NUMBER]
             [LEARNED]
             [LOCAL]
```

Where	Means
domain-name	This *domain-name* will be removed from the operational database.
ALL	All domain names known to the server be removed from the operational database.
ENTRY	Specifies that you will identify, by *entry-number* (see the SHOW/ MONITOR DOMAIN display, the *domain-name/internet-address* combination that will no longer be available to server users.
entry-number	The number of the *domain-name* shown in the "Entry" column of the SHOW/MONITOR DOMAIN display, which represents a *domain-name/internet-address* combination that will be removed from the operational database. Note that the number of an entry in the operational database does not need to match the entry number in the permanent database. Therefore, if you want to CLEAR and PURGE a domain-name, you should make sure that you have selected the correct entry number.
LEARNED	All *domain names* supplied by a Domain Name Server will no longer be available to server users, until the *domain names* are re-enabled with a SET DOMAIN command, learned from a Domain name server, or the server is re-initialized (for *domain names* that are contained in the permanent database).
LOCAL	All *domain names* that have been locally defined at the server (e.g., *domain names* specified using a SET DOMAIN command) will be removed from the operational database.

CLEAR/PURGE DOMAIN (continued)

Examples

```
CLEAR DOMAIN FINANCESUN.XYPLEX.COM

CLEAR DOMAIN LOCAL

CLEAR DOMAIN ENTRY 5
```

CLEAR IP SECURITY Privilege: P

This command enables a system manager to remove one or all entries from the Internet Security table in the operational database. Once cleared, an entry can be respecified using the SET PORT IP SECURITY command. If the entry is present in the permanent database, it will appear in the operational database again when the server is re-initialized. (Also refer to the PURGE IP SECURITY command, which is used to remove a security table entry from the permanent database.)

Refer to the Security Features section in the *Advanced Configuration Guide* for a description of Internet Security.

Examine the output of the SHOW/LIST PORT IP SECURITY command to determine the entry number in the Internet Security table that you want to remove. Note that security entries in the operational database do not need to match the entries in the permanent database. Therefore, if you want to CLEAR and PURGE a security entry, you should make sure that you have selected the correct entry number.

The server displays an error message if the entry you specify does not exist.

The CLEAR IP SECURITY command clears the security assignment (allow or deny access) for all ports in the *port-list*, for which the assignment was made. To disable Internet Security for a specific port, use the DISABLE option of the SET PORT IP SECURITY command.

Syntax

```
CLEAR IP SECURITY [entry-number]
                  [ALL]
```

Where	Means
entry	Corresponds to a number appearing in the Entry field of the SHOW/LIST PORT IP SECURITY display.
ALL	Clears all entries in the Internet Security table.

Example

```
CLEAR IP SECURITY 3
```

CLEAR PARAMETER SERVER Privilege: P

Use the CLEAR PARAMETER SERVER command to temporarily remove a specific parameter server from the list of available parameter servers. Typically, you would use this command to remove a parameter server, when the parameter server is no longer available. Because the parameter server is removed from the list of eligible parameter servers, the server will not update the parameter settings that are stored at the parameter server as these settings are changed. You can use the SHOW PARAMETER SERVER command to determine if a particular node is currently a parameter server for the server.

Note that the server may return the removed parameter server back to the list of eligible parameter servers the next time it does a check for eligible parameter servers. (This occurs at the frequency specified by the SET PARAMETER SERVER CHECK characteristic, or when the server manager issues a CHECK PARAMETER SERVER command. Also, whether the deleted parameter server returns to the list of eligible parameter servers maintained by the server is subject to the limit defined by the SET SERVER PARAMETER SERVER LIMIT command) To remove a parameter server permanently from the list of eligible parameter servers maintained by the server, you must disable the parameter server software (e.g., xyp_manager, BOOTP, TFTP, etc.) that is running at the node, remove the parameter server node from the network, or shut the node down.

For units which store parameters locally in Non-Volatile Storage (NVS), you cannot CLEAR the local parameter server.

Syntax

```
CLEAR PARAMETER SERVER <node name>
```

Where	Means
node name	The name of a node where server parameters have been stored, which is to be removed from the list of eligible parameter servers for the server.

Example

```
CLEAR PARAMETER SERVER NETWORKVAX
```

CLEAR PORT IP SECURITY Privilege: P

Use this command to remove Internet security entries for one or more designated port(s) from the operational database.

This command removes all Internet security entries pertaining to the designated port(s) from the Internet Security table in the operational database. Once cleared, an operational database entry can be respecified using the SET PORT IP SECURITY command. If the entry is present in the permanent database, it will appear in the operational database again when the server is re-initialized.

Refer to the Security Features section of the *Advanced Configuration Guide* for a description of the Internet Security feature.

Syntax

```
CLEAR PORT [port-list] IP SECURITY
```

Where	Means
port-list	One or more access server ports where all security entries will be removed.

Example

```
CLEAR PORT 4 IP SECURITY
```

CLEAR/PURGE PORT IPX RIP EXPORT Privilege: P

Use these commands to remove RIP export filters that you have previously created for one or more ports. See Using TCP/IP Features in the *Advanced Configuration Guide* for more information.

When the IPX protocol is enabled, the server advertises IPX RIP routes in its IPX route table to other IPX routers by default. This process is called *exporting*. You can define filters that prevent or allow individual ports from exporting routes. The export filter rules specify whether routes in the route table are "advertised" or "hidden." You can apply filters to specific networks or to ranges of networks.

Syntax

```
CLEAR/PURGE PORT port-list IPX RIP EXPORT [ALL]
                                          [NETWORK [network] [ALL]]
```

Where	Means
ALL	Remove all RIP export filters for the ports.
NETWORK	Remove only the RIP export filters that apply to a specific network or range of networks.
network	An IPX RIP network number. This is a hexadecimal value from 1 to FFFFFFFE. You can also specify ALL if you want the change to affect RIP import filters for all IPX networks.

Example

```
CLEAR PORT 5 IPX RIP EXPORT ALL

PURGE PORT ALL IPX RIP EXPORT NETWORK 1234

PURGE PORT ALL IPX RIP EXPORT NETWORK ALL
```

CLEAR/PURGE PORT IPX RIP IMPORT Privilege: P

Use these commands to remove RIP import filters that you have previously created for one or more ports. See Using TCP/IP Features in the *Advanced Configuration Guide* for more information.

By default, when the IPX protocol is enabled, a server adds all routes that it learns through RIP to its IPX route table. This process is called *importing*. You can define filters that prevent or allow individual ports from learning routes. The import filter rules specify whether routes in the route table are "accepted" or "discarded." You can apply filters to specific networks or to ranges of networks.

Syntax

```
CLEAR/PURGE PORT port-list IPX RIP IMPORT [ALL]
                                          [NETWORK [NETWORK] ]
                                                   [ALL]
```

Where	Means
ALL	Remove all RIP import filters for the ports.
NETWORK	Remove only the RIP import filters that apply to a specific network or range of networks.
network	An IPX RIP network number. This is a hexadecimal value from 1 to FFFFFFFE. You can also specify ALL if you want the change to affect RIP import filters for all IPX networks.

Examples

```
CLEAR PORT 5 IPX RIP IMPORT ALL

PURGE PORT ALL IPX RIP IMPORT NETWORK 1234

PURGE PORT ALL IPX RIP IMPORT NETWORK ALL
```

CLEAR/PURGE PORT IPX SAP EXPORT NETWORK Privilege: P

Use this command to remove SAP export filters that you have previously created for one or more ports. See Using TCP/IP Features in the *Advanced Configuration Guide* for more information.

By default, when the IPX protocol is enabled, an access server advertises all service Names and Types in its SAP table to other IPX routers. This process is called *exporting*. You can define filters that allow the server to export SAP service Names and Types or prevent the server from exporting them. The export filter rules specify whether service Names and Types are "advertised" or "hidden." You can apply SAP filters to specific networks or to types of SAP services.

Syntax

```
CLEAR/PURGE PORT [port-list] IPX SAP EXPORT NETWORK [network]TYPE [type-value]
                                                    [ALL]         [ALL]
```

Where	Means
NETWORK	Remove only the SAP export filters that apply to a specific network or range of networks.
network	An IPX SAP network number which is advertised or hidden by the port. This is a hexadecimal value from 1 to FFFFFFFE. You can also specify ALL if you want the change to affect SAP export filters for all IPX networks.
TYPE	Remove only the filters affecting certain SAP Service Types that are advertised or hidden by the port(s). These are specified by the following *type-value*(s):

type-value

type-value	**Description**
0	Unknown
1	User
2	User Group
3	Print Queue
4 or 278	File Server
5	Job Server
6	Gateway
7	Print Server
8	Archive Queue
9	Archive Server
A	Job Queue
B	Administration
24	Remote Bridge Server
47	Advertising Printer Server
107	Server (internal)

ALL	Remove all filters affecting SAP Service Types that are advertised or hidden by the port(s).

CLEAR/PURGE PORT IPX SAP EXPORT (continued)

Examples

```
PURGE PORT 5 IPX SAP EXPORT NETWORK ALL TYPE ALL
```

CLEAR/PURGE PORT IPX SAP IMPORT NETWORK Privilege: P

Use these commands to remove SAP import filters that you have previously created for one or more ports. See Using TCP/IP Features in the *Advanced Configuration Guide* for more information.

By default, when the IPX protocol is enabled, a Xyplex Access Server adds all service "Names" and "Types" that it learns through the Service Advertisement Protocol (SAP) to its IPX SAP table. This process is called *importing*. You can define filters that prevent the server from importing or exporting service Names and Types. Import filter rules specify whether service Names and Types learned through SAP are "accepted" or "discarded."

Syntax

```
CLEAR/PURGE PORT port-list IPX SAP IMPORT NETWORK [network] TYPE [type-value]
                                                  [ALL]           [ALL]
```

Where	Means
NETWORK	Remove only the SAP import filters that apply to a specific network or range of networks.
network	An IPX SAP network number which is accepted or discarded by the port. This is a hexadecimal value from 1 to FFFFFFFE. You can also specify ALL if you want the change to affect SAP export filters for all IPX networks.
TYPE	Remove only the filters affecting certain SAP service Types that are accepted or discarded by the port(s). These are specified by the following *type-value*(s):

type-value

type-value	**Description**
0	Unknown
1	User
2	User Group
3	Print Queue
4 or 278	File Server
5	Job Server
6	Gateway
7	Print Server
8	Archive Queue
9	Archive Server
A	Job Queue
B	Administration
24	Remote Bridge Server
47	Advertising Printer Server
107	Server (internal)

ALL	Remove all filters affecting SAP Service Types that are accepted or discarded by the port(s).

CLEAR/PURGE PORT IPX SAP IMPORT NETWORK (continued)

Example

```
PURGE PORT 5 IPX SAP IMPORT NETWORK ALL TYPE B
```

CLEAR/PURGE SERVER LPD QUEUE Privilege: P

Use this command to remove an entire LPD queue and cancels any print jobs currently in the queue. If you use the CLEAR/PURGE SERVER LPD QUEUE command, you should probably update the LPD configuration at any hosts that had access to the queue (i.e., edit the /etc/printcap command to remove the printer associated with the LPD queue at the server).

Use the REMOVE LPD QUEUE command to delete a specific job from the queue, without deleting the other jobs or the queue.

See Setting Up UNIX Daemons in the *Advanced Configuration Guide* for more information. See also the *ULI Guide* for a description of the lpc, lpq, and lprm commands that are available at the access server.

Syntax

```
CLEAR/PURGE SERVER LPD QUEUE ["queue-name"]
                             [ALL]
```

Where	Means
queue-name	The name of the LPD queue that you are removing. The name can be up to 16 characters long, and is case sensitive. Enclose the name in double-quotation marks (").
ALL	Remove all LPD queues.

Examples

```
CLEAR LPD QUEUE "line-printer"

PURGE LPD QUEUE ALL
```

CLEAR SERVER CCL NAME Privilege: P

CCL scripts are ASCII text files which contain commands that specify initialization and operational characteristics for the specific type of modem that is connected to a port. CCL scripts are stored at script servers (hosts which can transfer a file to the server via TFTP). Individual ports can be configured to use a specific CCL script using the DEFINE PORT CCL NAME command.

Occasionally, you may want to change the name of the CCL script assigned to some ports or stop using a certain CCL script altogether (this is called "unloading" a CCL script.). The CLEAR SERVER CCL NAME command causes the server to unload the CCL script *ccl-name* and free the associated memory. This command will fail if any ports are currently running the CCL script *ccl-name*.

Syntax

```
CLEAR SERVER CCL NAME "ccl-name"
```

Where	Means
ccl-name	The name of the CCL script to be unloaded from ports that use this script.

Example

```
CLEAR SERVER CCL NAME "SupraFAXModem_V.32bis"
```

CLEAR SERVER IP ROTARY Privilege: P

Use the CLEAR SERVER IP ROTARY command to delete, from the operational database, one or more internet rotary entries known by the server. (A rotary is a group of ports on the server which are assigned the same internet-address.) If the rotary is listed in the permanent database, it will again be made available when the server is re-initialized. (*See also* the PURGE SERVER IP ROTARY command.)

Use SHOW/MONITOR SERVER IP ROTARY command to determine the entry number for a particular rotary in the operational database. Note that when you remove an internet rotary entry from the database, the remaining internet rotary entries in the database are not renumbered. Also, internet rotary entries in the operational database do not need to match the entries in the permanent database. Therefore, if you want to CLEAR and PURGE a rotary, you should make sure that you have selected the correct entry number.

The server will display an error message if you use the CLEAR SERVER IP ROTARY command when the specified entry does not exist.

SYNTAX `CLEAR SERVER IP ROTARY [`*`ENTRY`*`]`
`[ALL]`

Where	**Means**
entry	Specifies the rotary entry number of the internet rotary that will be removed from the operational database.
ALL	Specifies that all internet rotaries known to the server will be removed from the operational database.

Examples

```
CLEAR SERVER IP ROTARY 1

CLEAR SERVER IP ROTARY ALL
```

CLEAR SERVER IP ROUTE Privilege: P

Use the CLEAR SERVER IP ROUTE command to delete, from the operational database, one or more internet-route entries known by the server. If the internet-route is listed in the permanent database, it will again be made available when the server is re-initialized. (Refer also to the description of the PURGE SERVER IP ROUTE command.)

Examine the SHOW/MONITOR SERVER IP ROUTE display to determine the entry number for a particular internet route in the operational database. Note that when you remove an internet route entry from the database, the remaining internet route entries in the database are not renumbered. Also, internet-route entries in the operational database do not need to match the entries in the permanent database. Therefore, if you want to CLEAR and PURGE an internet-route, you should make sure that you have selected the correct entry number.

The server will display an error message if you use the CLEAR SERVER IP ROUTE command when the specified entry does not exist.

Syntax

```
CLEAR SERVER IP ROUTE [ENTRY]
                      [ALL]
```

Where	Means
entry	Specifies the entry number of the internet-route that will be removed from the operational database.
ALL	Specifies that all internet-routes known to the server that will be removed from the operational database.

Examples

```
CLEAR SERVER IP ROUTE 1

CLEAR SERVER IP ROUTE ALL
```

CLEAR SERVER IP TRANSLATION TABLE Privilege: P

In an Ethernet local area network, all packets are addressed to their destinations with an Ethernet address. Therefore, for an Internet network running over an Ethernet network, an Internet addresses must be translated to its corresponding Ethernet address. During the course of normal server operations, the server inquires from other hosts on the network about which Ethernet address corresponds to a given Internet address. As a unit acquires Internet-to-Ethernet address translations, it stores them in a table in the operational database. (This table is usually referred to as the ARP table.) The operational database of a unit that runs TCP/IP-LAT software can store up to 60 of the most recently used Internet-to-Ethernet address translations.

Use this command to delete, from the operational database, one or more Internet-to-Ethernet address translation entries known by the unit. The translation will again be made available when it is relearned by the unit.

Examine the SHOW/MONITOR SERVER IP TRANSLATION TABLE display to determine the entry number for a particular internet route in the operational database. Note that when you remove an entry from the database, the remaining entries in the database are not renumbered.

The unit displays an error message if you use the CLEAR SERVER IP TRANSLATION TABLE command when the specified entry does not exist.

Syntax

```
CLEAR SERVER IP TRANSLATION TABLE [ENTRY-NUMBER]
                                  [ENTRY-RANGE]
                                  [ALL]
```

Where	Means
entry-number	The entry number (use the SHOW/MONITOR SERVER IP TRANSLATION TABLE command to display the current entries) of the translation that will be removed from the operational database.
entry-range	Enter a list of two or more consecutive *entry-numbers* from the SHOW/MONITOR SERVER IP TRANSLATION TABLE display, that will be removed from the operational database of the unit. The unit can relearn the translations. You can specify an entry-range by entering a range of *entry-numbers* separated by a hyphen or comma. For example, the entry-list 1, 3-5 refers to the individual entries: 1, 3, 4, and 5.

CLEAR SERVER IP TRANSLATION TABLE (continued)

ALL	All translations known to the unit will be removed from the operational database of the unit. The unit can relearn the translations.

Examples

```
CLEAR SERVER IP TRANSLATION TABLE 1

CLEAR SERVER IP TRANSLATION TABLE ALL

CLEAR SERVER IP TRANSLATION TABLE 1,3-5
```

CLEAR/PURGE SERVER IPX RIP EXPORT Privilege: P

The server advertises all routes in its IPX route table to other IPX routers, by default. This process is called *exporting*.

SYNTAX `CLEAR/PURGE SERVER IPX RIP EXPORT [NETWORK] [`*`NETWORK`*`]`
`[ALL]`

Where	Means
ALL	All routes in the server's route table will be removed.
NETWORK	Clears a specific network when a source or destination network is included.
network	A hexadecimal value from 1 to FFFFFFFE.

Example

```
CLEAR SERVER IPX RIP EXPORT NETWORK ALL
```

CLEAR/PURGE SERVER IPX RIP IMPORT Privilege: P

When the IPX protocol is enabled, the access server adds all routes that it learns through RIP to its route table by default.

Syntax

```
CLEAR/PURGE SERVER IPX RIP IMPORT [NETWORK [network] ]
                                  [ALL]
```

Where	Means
ALL	All networks will be cleared.
NETWORK	Clears a specific network when a source or destination network is included.
network	A hexadecimal value from 1 to FFFFFFFE.

Example

```
CLEAR SERVER IPX RIP IMPORT NETWORK ALL
```

CLEAR/PURGE SERVER IPX SAP EXPORT NETWORK Privilege: P

Clears all service Names and Types in the server's SAP table to other IPX routers.

Syntax

```
CLEAR/PURGE SERVER IPX SAP EXPORT NETWORK [NETWORK]
                                          [ALL]
```

Where	Means
NETWORK	Clears a specific network when a source or destination network is included.
network	The source or destination network to purge. Enter a hexadecimal value from 1 to fffffffe.
ALL	Clears all service names and types from all networks.

Example

```
PURGE SERVER IPX SAP EXPORT NETWORK ALL
```

CLEAR/PURGE SERVER IPX SAP EXPORT TYPE Privilege: P

Clears all NetWare service types such as file server or printer from either a specific NetWare network or all NetWare networks.

Syntax

```
CLEAR/PURGE SERVER IPX SAP EXPORT TYPE [type-value]
                                       [ALL]
```

Where	Means

type-value

Service Type	Description
0	Unknown
1	User
2	User Group
3	Print Queue
4 or 278	File Server
5	Job Server
6	Gateway
7	Print Server
8	Archive Queue
9	Archive Server
A	Job Queue
B	Administration
24	Remote Bridge Server
47	Advertising Printer Server
107	Server (internal)

ALL — Purges all service types.

Example

```
PURGE SERVER IPX SAP EXPORT TYPE ALL
```

CLEAR/PURGE SERVER IPX SAP IMPORT NETWORK Privilege: P

Clears all service types and names that were learned through SAP from its IPX SAP table.

Syntax

```
CLEAR/PURGE SERVER IPX SAP IMPORT NETWORK [NETWORK]
                                          [ALL]
```

Where	Means
network	Clears all service types from a specific network. Enter a hexadecimal value from 1 to fffffffe.
ALL	Clears all service types from all NetWare networks.

Example `PURGE SERVER IPX SAP IMPORT NETWORK ALL`

CLEAR/PURGE SERVER IPX SAP IMPORT TYPE Privilege: P

Clears all NetWare service types such as file server or printer that were learned through SAP from its IPX SAP table from either a specific NetWare network or all NetWare networks.

Syntax `CLEAR/PURGE SERVER IPX SAP IMPORT TYPE [`*TYPE-VALUE*`]`
`[ALL]`

Where	Means
type-value	**NetWare Service Type** / **Description**

NetWare Service Type	Description
0	Unknown
1	User
2	User Group
3	Print Queue
4 or 278	File Server
5	Job Server
6	Gateway
7	Print Server
8	Archive Queue
9	Archive Server
A	Job Queue
B	Administration
24	Remote Bridge Server
47	Advertising Printer Server
107	Server (internal)

ALL	Clears all NetWare service types learned from all networks.

Example

```
PURGE SERVER IPX SAP IMPORT TYPE ALL
```

CLEAR SERVER MENU Privilege: P

This command enables a system manager to remove an item on the server's menu from the operational database. Once cleared, the entry can be respecified using the SET SERVER MENU command. If the entry is present in the permanent database, it will appear in the operational database again when the server is re-initialized. (Also refer to the PURGE SERVER MENU command, which is used to remove a menu item from the permanent database.)Examine the output of the SHOW/LIST SERVER MENU command to determine the number of the entry you want to remove. The server will display an error message if the entry you specify does not exist.

See the Menu section of *Basic Configuration Guide* for a description of the Simple Menu Interface feature.

Syntax

```
CLEAR SERVER MENU [item-number]
```

Where	Means
item-number	Specifies the item number (1 - 20) within the menu that you want to clear.

Example

```
CLEAR SERVER MENU 3
```

CLEAR SERVER SCRIPT SERVER Privilege: P

Use this command to delete, from the operational database, one or more script servers, where the server attempts to locate script files. If the script server is listed in the permanent database, it will again be made available when the server is re-initialized. (*See also* the PURGE SERVER SCRIPT SERVER command.)

Examine the SHOW/MONITOR SERVER SCRIPT SERVER display to determine the entry number for a particular script server in the operational database. Note that when you remove an script server entry from the database, the remaining script server entries in the database are not renumbered. Also, script server entriesin the operational database do not need to match the entries in the permanent database. Therefore, if you want to CLEAR and PURGE an script server, you should make sure that you have selected the correct entry number.

The server will display an error message if you use the CLEAR SERVER SCRIPT SERVER command when the specified entry does not exist.

Syntax

```
CLEAR SERVER SCRIPT SERVER [entry-number]
                           [ALL]
```

Where	Means
entry-number	Remove this script server entry from the operational database.
ALL	Remove all script servers known to the server from the operational database.

Examples

```
CLEAR SERVER SCRIPT SERVER 1

CLEAR SERVER SCRIPT SERVER ALL
```

CLEAR SERVICES — Privilege: P

Use this command to delete, from the operational database, an entry for one or all of the LAT services offered locally at the server. You can use the SET SERVICE command to re-enable the deleted service. If the service is listed in the permanent database, the service will again be made available when the server is re-initialized. (See also the PURGE SERVICES command.)

The server will display an error message if you use the CLEAR SERVICES command when sessions are cuurently established with the service(s) to be deleted, when there are connection requests in the connection queue for the service(s), or when the specified service does not exist.

Syntax

```
CLEAR SERVICES [service-name]
               [LOCAL]
```

Where	Means
service-name	Remove this local LAT service (e.g., a service which is offered by the server) from the operational database.
LOCAL	Remove all local services (e.g., services which are offered by the server) from the operational database.

Examples

```
CLEAR SERVICES LOCAL

CLEAR SERVICES LASER_PRINTER
```

CLEAR XPRINTER PORTS Privilege: P

Use the CLEAR XPRINTER PORTS command to disconnect ports temporarily from the Novell print servers to which they are connected.

SYNTAX

```
CLEAR XPRINTER PORTS [port-list]
                     [ALL]
```

Where	Means
port-list	Terminate Novell client printing at one or more terminal or Xyplex printer server ports.
ALL	Terminate Novell client printing at all ports which offer this service.

Example

```
CLEAR XPRINTER PORTS 1,3-5
```

CLEAR XPRINTER Privilege: P

Use this command to temporarily remove a Novell printer server from the list of active print servers that the Xyplex unit maintains. Once per minute, an active Novell print server broadcasts a message on to the network to indicate that it is "alive." This means that the Xyplex unit will re-learn the print server until you also unload it from the NetWare file server or print server workstation.

Syntax

```
CLEAR XPRINTER [printer-server]
```

Where	Means
printer-server	Remove the Novell NetWare printer server that is serviced by the Xyplex unit.

Example

```
CLEAR XPRINTER LASER
```

CONNECT Privilege: S, N, P

Use this command to establish a session by creating a virtual connection between your port (terminal) and a LAT service that is offered at a service node, or a Telnet destination. Most users will use the CONNECT command to establish a session between the port they are logged on to and a host When you use CONNECT without specifying a *service-name*, the access server tries to establish a session with a LAT preferred service or with the preferred Telnet destination (domain-name or internet-address, and telnet-port number), when any of these are defined.

In networks where both LAT services and Telnet destinations exist, the access server establishes sessions between the port and the LAT service or Telnet destination based on the setting of the PORT RESOLVE SERVICE. If this setting is set to LAT, the access server interprets all command qualifiers as applicable to LAT services. In this case, the access server attempts to locate the service, specified by the *service-name*, among LAT service nodes. If the characteristic is set to Telnet, the access server interprets all CONNECT command qualifiers as applicable to Telnet destinations. In this case, the access server attempts to connect to a Telnet *domain-name/ internet-address* and *telnet-port number*. If the characteristic is set to ANY_LAT, ANY_TELNET, the access server first attempts to connect to a LAT service, then to a Telnet *domain-name/internet-address* and *telnet-port number*. (Regardless of the setting of the PORT RESOLVE SERVICE characteristic, you can require the access server to interpret CONNECT command qualifiers as applicable to either LAT or Telnet, by using the LAT or TELNET keyword. See also the LAT CONNECT and TELNET CONNECT commands).

Connections to a LAT service are also subject to the following conditions:

1. Both the port and the device offering the LAT service must have a matching authorized group code.

2. When a service that is offered at a access server port is busy, additional connection requests are entered into a connection queue, if the SET SERVICE QUEUE characteristic is set to ENABLED.

LAT services can be offered at more than one LAT service node or port. The access server assumes that all services which have the same *service-name* are equivalent. Therefore, when a service is offered at more than one node or port, the access server connects to the node or port which has the highest rating (the relative ability to support additional connections). CONNECT command options permit you to select the particular service node or port, where the service is offered, to which the access server connects.

Connect (continued)

Syntax

```
CONNECT [[SERVICE] service-name] [NODE node name] [DESTINATION port name] [CONTROLLED]
[domain-name[:telnet-port number]]
[internet-address[:telnet-port number]]
```

Where	Means
SERVICE	Use this option when you provide a *service-name* to which the port will be connected.
service-name	The name of the LAT service to which the port will be connected.
NODE	Use this option when you provide the name of the service node that offers the service specified by the *service-name*. Use this keyword when a service is offered at more than one service node.
node name	The LAT node which offers the service specified by the *service-name*.
DESTINATION	You will provide the name of the access server port at which the service, specified by the *service-name*, is offered. Use this keyword when a service is offered at more than one port.
port name	The port on the access server that offers the service specified by the *service-name*.
CONTROLLED	Frames a session with strings specified with the DEFINE/SET PORT CONTROLLED SESSION INITIALIZE/TERMINATE command.
domain-name	The logical name of the Telnet destination that will be the connection partner in a session with the target port. If the specified *domain-name* is not a fully qualified *domain-name*, the name will be concatenated with the default *Internet domain-name-suffix*. Note that the first time the server attempts to connect to any *domain-name* (following initialization), a connection takes 2 seconds because the server must locate a Domain Name Server and then attempt the connection. Subsequent attempts to connect to a *domain-name* occur without delay, because the server already knows the location of a Name Server.
internet-address	The location on the network of the Telnet destination that will be the connection partner in a session with the target port.
:telnet-port number	The number of the target Internet protocol or physical port number that is used in the session between the target port and the connection partner (i.e., host or access server). Note that the colon character (:) is required to separate the *telnet-port number* from the *domain-name* or *internet-address*.

Connect (continued)

Examples

```
CONNECT FINANCEVAX CONTROLLED
```

```
CONNECT 140.179.244.38:3800
```

Establish a session between this port and Telnet destinationwhose *internet-address* is 140.179.244.38. Note that the user specified a *telnet-port number* (3800 in this case).

```
CONNECT FINANCEVAX:23
```

CONNECT PORT Privilege: P

Users at privileged ports can establish sessions between a port, other than the port they are logged on to, and a LAT service or Telnet destination. Use the CONNECT PORT command to establish a session by creating a virtual connection between an access server port, called the "target" port and a LAT service or a Telnet destination, or another port on an access server. The target port is usually a port other than the port you are currently logged on to.

To use this command, you must specify the name of a LAT service or Telnet destination. This can be done either by the CONNECT PORT command, or by defining a dedicated or preferred service for the target port. The target port cannot have a session in progress (you can terminate an active session using the DISCONNECT PORT or LOGOUT PORT command).

In networks where both LAT services and Telnet destinations exist, the access server will establish sessions between the port and the LAT service or Telnet destination based on the setting of the PORT RESOLVE SERVICE characteristic. If this characteristic is set to LAT, the access server will interpret all command qualifiers as applicable to LAT services. In this case, the access server will attempt to locate the service, specified by the *service-name*, among LAT service nodes. If the characteristic is set to Telnet, the access server will interpret all CONNECT command qualifiers as applicable to Telnet destinations. In this case, the access server will attempt to connect to a Telnet *domain-name/internet-address* and *telnet-port number*. If the characteristic is set to ANY, the access server will first attempt to connect to a LAT service, then to a Telnet destination (*domain-name* or *internet-address* and *telnet-port number*). Regardless of the setting of the PORT RESOLVE SERVICE characteristic, you can require the access server to interpret CONNECT command qualifiers as applicable to either LAT or Telnet, by using the LAT or TELNET keyword. See also the LAT CONNECT and TELNET CONNECT commands.

LAT services can be offered at more than one service node or port. The access server assumes that all services which have the same *service-name* are equivalent. Therefore, when a service is offered at more than one LAT service node or port, the access server will connect to the node or port which has the highest rating (the relative ability to support additional connections). CONNECT PORT command options permit you to select the particular service node or port, where the service is offered, to which the access server will connect.

Syntax

```
CONNECT PORT port number [service-name] [NODE node name] [DESTINATION port number]
                         [domain-name[:telnet-port number]]
                         [internet-address[:telnet-port number]]
```

CONNECT PORT (continued)

Where	Means
PORT	You will connect a target port to a LAT service or Telnet destination.
port number	The port number of the target access server port which will be connected to a LAT service or Telnet destination.
service-name	The LAT service to which the target access server port, specified by the *port number* will be connected.
NODE	You will designate a LAT node that offers the service specified by the *service-name*. Use this keyword when there are multiple LAT service nodes which offer the service.
node name	The LAT service node which offers the service specified by the *service-name*.
DESTINATION	You will designate a access server port which offers the service specified by the *service-name*. Use this keyword when there are multiple access server ports which offer the service.
port name	The access server port which offers the service, specified by the *service-name*.
domain-name	The logical name of the Telnet destination that will be the connection partner in a session with the target port. If the specified *domain-name* is not a fully qualified *domain-name*, the specified name will be concatenated with the default Internet *domain-name-suffix*. Note that the first time the server attempts to connect to any *domain-name* (following initialization) takes 2 seconds to occur because the server must locate a Domain Name Server and then attempt the connection. Subsequent attempts to connect to a *domain-name* occur without delay, because the server already knows the location of a Name Server.
internet-address	The location on the network of the Telnet destination that will be the connection partner in a session with the target port.
:telnet-port number	The number of the target Internet protocol or physical port number that is used in the session between the target port and the connection partner. Note that the colon character (:) is required to separate the *telnet-port number* from the *domain-name* or *internet-address*.

CONNECT PORT (continued)

Examples

```
CONNECT PORT 5 128.10.2.30:23

CONNECT PORT 5 LASER NODE MAX1620 DESTINATION PORT_2
```

CRASH Privilege: P

Use this command to require the server to execute a "crash dump" procedure when a problem occurs. During a crash dump procedure, the server sends a copy of the contents of its memory to a "dump file" at the dump server (when the SERVER DUMP is ENABLED) by Xyplex Customer Support for analysis, and then the server re-initializes. When you use the CRASH command, users will not have access to the server until the server re-initializes (users will have to logon and re-connect).

Syntax

CRASH

Example

CRASH

DEFINE and SET Commands

Use the DEFINE and SET commands to specify or change settings for domain names, ports or terminals, servers, services, and user privilege levels. The differences between the two commands are as follows:

DEFINE Command	SET Command
Changes the settings within the permanent database.	Changes the settings only for the operational database.
Changes do not take effect immediately, but are stored in the permanent database so they remain in effect whenever the access server is re-initialized.	The permanent settings are not altered. Any parameters that have been defined via the SET command are not retained, when the access server is re-initialized.
Use the DEFINE SERVER CHANGE ENABLED command to cause the changes to take effect immediately and on a permanent basis.	Use the SET SERVER CHANGE ENABLED command to cause the changes to take effect immediately and on a permanent basis.

Domain names that are entered into the databases via a SET/DEFINE DOMAIN command are called locally defined domain names

Domain names that are listed in the permanent database (i.e., using the DEFINE DOMAIN command) are entered into the operational database whenever the access server is re-initialized.

In addition to the locally defined *domain names*, the access server can use *domain names* that it obtains from one or more DNS server in the network. These *domain names* are only entered into the operational database. *Domain names* that are entered into the databases via a DNS server are called "learned" *domain names*.

Each domain-name can be assigned up to 16 *internet addresses* (this is called a rotary group). The operational database can contain a maximum of 100 *domain name/internet address* combinations. (However, if you are using a DNS server, you should not specify more than 99 *domain name/internet address* combinations, or the server will not be able to learn any *domain names*.)

Locally defined domain names stay in the operational database until they are removed via a CLEAR/PURGE DOMAIN command. The access server keeps a *learned* domain name in the operational database until:

- it is removed via a CLEAR DOMAIN command, or
- the expiration of a period of time (time to live) that is assigned by the DNS server. The TCP/IP-LAT software limits the time to live to the setting of the SERVER IP DOMAIN TTL, or
- the operational database contains the maximum number of *domain names*, and a user adds a new *domain-name* via a SET DOMAIN command, or the access server learns a new *domain-name* from a DNS server. In this case, the access server replaces the oldest learned *domain-name* in the operational database with the new name.

See the Using the TCP/IP Features section of the *Advanced Configuration Guide* for information about setting up a server to perform domain name serving.

DEFINE/SET DOMAIN Commands (continued)

Syntax

```
DEFINE/SET DOMAIN [domain-name] [internet-address]
```

Where	Means
domain-name	If the specified *domain-name* is not a fully qualified *domain-name*, the specified name will be concatenated with the default Internet *domain-name-suffix*.
internet-address	The internet-address of the *domain-name*.

Examples

```
DEFINE DOMAIN UNIXSUN.COM 192.112.119.210
```

DEFINE/SET PORT - General Information

The DEFINE/SET PORT commands specify or modify port settings. Generally, port settings control communication between the server and the devices (e.g., terminals, modems, printers) which are connected to the server on the serial port. Changes that are made using the SET PORT command take effect immediately, but only remain in effect until the port is logged out. Changes that are made using the DEFINE PORT commandtake effect the next time the port is logged out, or when the server is re-initialized. Changes can be made to take effect both immediately and on a permanent basis when you set the SERVER CHANGE command to ENABLED.

Some port settings can only be set by users at privileged ports (there is more information on this in the Syntax section below). Whether or not a command is available to non-privileged or secure users, only privileged users can specify settings for ports other than their own port. Secure users can only issue SET PORT commands.

Syntax

The basic syntax for the DEFINE PORT and SET PORT commands is:

```
DEFINE/SET PORT [port-list] [characteristics]
                [ALL]
```

Where	Means
port-list	A list of one or more access server ports numbers.
ALL	Use this setting for all ports on the server.

As shown above, you can define or set multiple port characteristics with a single command. When you specify more than one port characteristic with one command, separate the characteristics with one or more spaces, a comma, or any combination of commas and spaces. (Note, however, that the maximum length of a command line is 132 characters.) You can use the word "TERMINAL" interchangeably with the word "PORT."

The common variables are listed in this section. The common variables are listed at the beginning of this book.

Valid DEFINE/SET PORT Commands

Command DEFINE/SET PORT	Define	Set
ACCESS	X (P)	X (P)
ALTERNATE NONE	X	X
ALTERNATE SPEED	X (P)	X (P)
APD	X (P)	X (P)
ARAP	X (P)	X (P)
AUTHORIZED GROUP	X (P)	X (P)
AUTOBAUD	X (P)	X (P)
AUTOCONNECT	X	X
AUTODEDICATED	X (P)	X (P)
AUTOHANGUP	X (P)	X (P)
AUTOPROMPT	X	X
BACKWARDS	X	X
BREAK REMOTE	X (L)	X (L)
BREAK LOCAL	X (L)	X (L)
BREAK LENGTH	X (L)	X (L)
BROADCAST	X	X
CCL AUDIBLE	X (P)	X (P)
CCL INAUDIBLE	X (P)	X (P)
CCL MODEM	X (P)	X (P)
CCL NAME	X (P)	X (P)

CHARACTER SIZE	X (L)	X (L)
CLEAR IP SECURITY ENTRIES	X (P)	X (P)
COMMAND	X (P)	X (P)
CONNECT RESUME	X	X
CONTROLLED PORT LOGIN	X (P)	X (P)
DCD TIME OUT	X (P)	X (P)
DEDICATED SERVICES	X (P)	X (P)
DEFAULT SESSION MODE	X (P)	X (P)
DIALBACK	X (P)	X (P)
DIALUP	X (P)	X (P)
DIALOUT ACTION	X (P)	X (P)
DISCARD ERROR	X (P)	X (P)
DSRLOGOUT	X (P)	X (P)
DSRWAIT	X (P)	X (P)
DTRWAIT FORCONNECTION	X (P)	X (P)
DTRWAIT FORRING	X (P)	X (P)

P) - Privileged users. (L) - Local mode only — Not applicable

Valid DEFINE/SET PORT Commands (continued)

Command DEFINE/SET PORT	Define	Set
FLOW	X (L)	X (L)
FORWARDS	X	X
PORT FROM PORT	X (P)	X (P)
GROUPS	—	X
IDLE TIMEOUT	X (P)	X (P)
INACTIVITY	X (P)	X (P)
INPUT FLOW	X (L)	X (L)
INTERRUPT	X (P)	X (P)
IP CONNECTIONS	X (P)	X (P)
IP CSLIP	X (L)	X (L)
IP FILTER	X (P)	X (P)
IP FILTER DESTINATION	X (P)	X (P)
IP SECURITY	X (P)	X (P)
IP SLIP ADDRESS	X (P)	X (P)
IP SLIP INTERUPPTS	X (P)	X (P)
IP SLIP AUTOSEND	X (L)	X (L)
IP SLIP MASK	X (P)	X (P)
IP SLIP REMOTE	X (P)	X (P)
IP TCP KEEPALIVE	(X)P	X (P)
IP TCP OUTBOUND	X (P)	X (P)
IP TCP WINDOW SIZE	X (P)	X (P)

IPX FILTER DEST NETWORK MODE	X (L)	X (L)
IPX FILTER PACKET TYPE	X (L)	X (L)
IPX NETWORK	X (L)	X (L)
IPX REMOTE NODE	X (P)	X (P)
IPX RIP	X (P)	X (P)
IPX SAP	X (P)	X (P)
KERBEROS	X (P)	X (P)
KEYMAPS	(X)	(X)
LAT DEDICATED	X (P)	—
LAT PREFERRED	X (P)	X (P)
LIMITED VIEW	X (P)	X (P)
LINE EDITOR	X	X

(P) - Privileged users. (L) - Local mode only — Not applicable

Valid DEFINE/SET PORT Commands (continued)

Command DEFINE/SET PORT	Define	Set
LOCAL	X	X
LOGIN DURATION	X (P)	X (P)
LOSS	X	X
MENU	X (P)	X (P)
MESSAGE	X	X
MODEM	X (P)	X (P)
MULTISESSIONS	X (L)	X (L)
NAME	X (P)	X (P)
NESTED MENU	X (P)	X (P)
NOLOSS	X	X
OUT BOUNDSECURITY	X (P)	X (P)
OUTPUT FLOW	X (L)	X (L)
PARITY	X (L)	X (L)
PASSWORD	X (P)	X (P)
PASSWORD PROMPT	X	X
PAUSE	X	X
PPP ACTIVE	X (L)	X (L)
PPP CHAP CHALLENGE TIMER	X	—
PPP CHAP RADIUS	X (P)	X (P)
PPP CHARMAP	X (P)	X

PPP CONFIGURE LIMIT	X (L)	X (L)
PPP DEFAULTS	X (L)	X (L)
PPP FAILURE LIMITS	X (L)	X (L)
PPP IP BROADCAST	X (L)	X (L)
PPP IP LOCAL ADDRESS	X (L)	X (L)
PPP IP LOCAL ADDRESS RANGE	X (L)	X (L)
PP IP MASK	X (L)	X (L)
PPP IP REMOTE ADDRESS RANGE	X (L)	X (L)
PPP IP VJ COMPRESSION	X (L)	X (L)
PPP IPX FILTER	X (L)	X (L)
PPP IPX NETWORK	X (L)	X (L)
PPP IPX NODE	X (L)	X (L)
PPP IPX REMOTE NODE	X (L)	X (L)
PPP IPX RIP	X (L)	X (L)
PPP IPX SAP	X (L)	X (L)

(P) - Privileged users. X (L) - Local mode only — Not applicable

Valid DEFINE/SET PORT Commands (continued)

Command DEFINE/SET PORT	Define	Set
PPP KEEPALIVE TIMEOUT	X (L)	X (L)
PPP KEEPALIVE TIMER	X (L)	X (L)
PPP LOGGING	X (L)	X (L)
PPP MAGIC NUMBER	X (L)	X (L)
PPP PAP KERBEROS	X (P)	X (P)
PPP PAP LOCAL	X (P)	X (P)
PPP PAP RADIUS	X (P)	X (P)
PPP RESTART TIMER	X (L)	X (L)
PREFERRED SERVICES	X (L)	X (L)
PRIVILEGED MENU	X (P)	X (P)
PRIVILEDGE NESTED MENU	X (P)	X (P)
PROMPT	X (P)	X
QUEUE	—	—
RADIUS ACCOUNTING	X (P)	X (P)
RADIUS SOLICITS	X (P)	X (P)
RESOLVE	X	X
RLOGIN	X (P)	X (P)
RLOGIN TRANSPARENT MODE	X (P)	X (P)
RLOGIN PREFERRED SERVICES	X (L)	X (L)
SCRIPT	X (P)	X (P)
SCRIPT ECHO	X (P)	X (P)

SCRIPT LOGIN	X (P)	X (P)
SECURID	X (P)	X (P)
SECURITY	X (P)	X (P)
SESSION LIMIT	X (P)	X (P)
SESSION MODE	X	X
SESSIONS	—	X
SIGNAL CHECK	X (P)	X (P)
SLIP IP MASK	X (P)	X (P)
SPEED	X	X
STOP BITS	X (P)	X (P)
TELNET	X (P)	X (P)
TELNET ABORT OUTPUT	X	X
TELNET ATTENTION	X	X
TELNET BINARY SESSION MODE	X	X
TELNET COMPORTCONTROL	X (P)	—
TELNET CSI ESCAPE	X	X

(P) - Privileged users. (L) - Local mode only — Not applicable

Valid DEFINE/SET PORT Commands (continued)

Command DEFINE/SET PORT	Define	Set
TELNET DEDICATED SERVICE	X (P)	—
TELNET DEDICATED SERVICE KICKSTART	X (P)	—
TELNET DEDICATED SERVICE USERDATA	X (P)	—
TELNET DEFAULT	X	X
TELNET DEFAULT LOCATION	X (P)	X (P)
TELNET DEFAULT TERMINALS	X (P)	X (P)
TELNET ECHO MODE	X	X
TELNET EOR REFLECTION	X (P)	X (P)
TELNET ERASE CHARACTER	X	X
TELNET ERASE LINE	X	X
TELNET INTERRUPT	X	X
TELNET INTERRUPTS AS BREAK	X (P)	X (P)
TELNET TERMINAL TYPES	X (P)	X (P)
TELNET NEWLINE	X	X
TELNET NEWLINE FILTERING	X	X
TELNET OPTION DISPLAY	X	X
TELNET PASS8D	X (P)	X (P)
TELNET PREFERRED SERVICE	X	X
TELNET QUERY	X	X
TELNET REMOTE	X (P)	X (P)
TELNET RS491	X (P)	X (P)

TELNET SYNCHRONIZE	X	X
TELNET TERMINAL TYPE	X	X
TELNET TRANSMIT	X	X
TELNET URGENT BREAK	X (P)	X (P)
TELNET TYPE	X	X
TELNET TYPEAHEAD SIZE	X (P)	X (P)
TELNET TN3270 DEFAULT PORT	X (P)	X (P)
TELNET TN3270 DEFAULT TERMINAL	X (P)	X (P)
TELNET TN3270 DEVICE	X (P)	X (P)
TELNET TN3270 EOR	X (P)	X (P)
TELNET TN3270 ERRORLOCK	X (P)	X (P)
TELNET TN3270 PREFIXKEYMAP	X (P)	X (P)
TELNET TN3270 PRINTER PORT	X (P)	X (P)
TELNET TN3270 SCANNER	X (P)	—

(P) - Privileged users. (L) - Local mode only — Not applicable

Valid DEFINE/SET PORT Commands (continued)

Command DEFINE/SET PORT	Define	Set
TELNET TN3270 SPACE INSERT	X (P)	—
TELNET TN3270 TRANSLATIONTABLE	X (P)	X (P)
TELNET TN3270 TYPE_AHEAD	X (P)	—
TELNET TN3270 XTDATTRS	X (P)	X (P)
ULI	X (P)	—
USER KERBEROS PASSWORD	X	X
USERNAME FILTERING	X	X
USERNAME PROMPT	X	X
VERIFICATION	X	X
WELCOME BEFORE AUTHENTICATION	X (P)	—
XDM HOST	X (P)	—
XDM QUERY	X (P)	X (P)
XON SEND TIMER	X (P)	—
XREMOTE	X (P)	—

(P) - Privileged users. (L) - Local mode only — Not applicable

DEFINE/SET PORT ACCESS Privilege: P

Use this command to specify the type of access permitted for the device using the port. If there is an active remote session in progress at a port when the ACCESS is SET for that port, and then the session is disconnected, the ACCESS setting will revert to the value defined in the permanent database. This operation is different on a DECserver Terminal Server.

***Note**: On some access servers you can access the local command mode from the LAN, only Xyplex Access Servers local command mode is only available on Port 0.*

Syntax

```
DEFINE/SET PORT port-list ACCESS   [DYNAMIC]
                                   [LOCAL]
                                   [NONE]
                                   [PRT3270]
                                   [REMOTE]
```

Where	Means
DYNAMIC	The port is accessible from either the local command mode or remotely by port number or by service name.
LOCAL	The port is accessible only by the local command mode from a serial connection only. This is the default.
NONE	The port is not accessible from either the local command mode, or remotely by port number or service name. This setting is often used for security on unused ports.
PRT3270	The port will be the TN3270 print screen client for this server. The port must have a TN3270 device assigned, and for each user's port the TN3270 device definition or keymap must include a PRINT key definition. This keyword is only valid when the TN3270 feature is enabled on the server. Do not use this option if you have enabled the server to logout when the DCD signal is deasserted. Use the SHOW PORT CHARACTERISTIC command to display the current setting of DSRLOGOUT. See also the DEFINE/SET PORT DSRLOGOUT command.
REMOTE	The device attached to the port is accessible only remotely by reverse-Telnet or by LAT service name.

Example

```
DEFINE PORT 1-5,20 ACCESS DYNAMIC
```

The server manager is defining the ACCESS for ports 1 through 5 and port 20.

DEFINE/SET PORT ALTERNATE SPEED Privilege:

Use this command to set the baud rate for the port(s).

Syntax

```
DEFINE/SET PORT <port-list> ALTERNATE SPEED <baud-rate>
```

Where	Means
baud-rate	Valid baud rates are: 50, 75, 110, 134, 150, 300, 600, 1200, 1800, 2000, 2400, 4800, 9600, 14400, 19200, 21600, 26400, 28800, 33600, and 38400 bits per second (baud rate). The device connected to the port must be set to one of these speeds

DEFINE PORT APD — Privilege: P

Automatic Protocol Detection (APD) applies only to dial-in connections. To use APD, the access server port must be configured with PORT ACCESS set to LOCAL or DYNAMIC.

Use this command to configure access server ports to accept connections made via different protocols, using the Automatic Protocol Detection (APD) feature. Using APD, ports will automatically determine the protocol being used to make a connection and adjust port settings appropriately. If you do not enable APD, ports can be dedicated for use by a single access serving protocol. An individual port can be configured to accept any connections made via ARAP, PPP, SLIP (which includes CSLIP), and interactive protocols, as well as all or none of these.

See the Using the TCP/IP Features section of the *Advanced Configuration Guide* for detailed information about how to configure servers and ports for APD.

Syntax

```
DEFINE PORT port-list APD [PROTOCOL LIST]    [ALL]
                                             [ARAP]
                                             [DISABLED]
                                             [INTERACTIVE]
                                             [NONE]
                                             [PPP]
                                             [SLIP]
```

Where	Means
protocol-list	You can include more than one protocol in the *protocol-list* (separate each protocol in the list with a comma).
ALL	Any type of connection can be established at the port(s).
ARAP	Port is limited to ARAP connection types.
DISABLED	The default is DISABLED, which is the same as NONE.
INTERACTIVE	Port is limited to INTERACTIVE connection types.
NONE	NONE is the same as DISABLED.
PPP	Port is limited to PPP connection types.
SLIP	Port is limited to SLIP connection types.

Example

```
DEFINE PORT 6-12 APD ARAP,PPP
```

DEFINE/SET PORT APD AUTHENTICATION Privilege: P

If the APD feature has been enabled on a port, use this command to determine when user authentication is implemented: either before or after APD determines the user protocol being used (such as INTERACTIVE, PPP, SLIP). APD authentication is required in addition to protocol-level authentication mechanisms. If authentication will be done after protocol detection, PPP or SLIP users must use a protocol-level authentication such as PAP or CHAP.

Syntax

```
DEFINE/SET PORT <port-list> APD AUTHENTICATION INTERACTIVE ONLY   [ENABLED]
                                                                  [DISABLED]
```

Where	Means
ENABLED	When this feature is enabled, the port will first determine the user protocol used when connecting. INTERACTIVE users will be prompted for username and password after entering Interactive mode (press <Return> four times). If it detects PPP or SLIP protocol, then protocol-level authentication such as PAP or CHAP (if enabled) will be used. If PAP or CHAP are not enabled on the port (not the dial-in client), the user will gain access without any security check.
DISABLED	If this feature is disabled, the user is first prompted for security authentication, then APD will check for the user protocol when connected. This is the default.

DEFINE/SET PORT APD DEFAULT Privilege: P

For ports where the APD features has been enabled, use this command to specify the action that the port(s) will take if the ports are unable to determine which protocol is being used to make a connection.

Access server ports can be configured to accept connections made via different protocols, using the Automatic Protocol Detection (APD) feature. Using APD, ports will automatically determine the protocol being used to make a connection and adjust port settings appropriately. Alternatively, by not enabling APD, ports can be dedicated for use by a single access serving protocol. An individual port can be configured to accept any connections made via ARAP, PPP, SLIP (which includes CSLIP), and interactive protocols, as well as all or none of these.

Syntax

```
DEFINE PORT port-list APD DEFAULT   [LOGOUT]
                                    [ARAP]
                                    [PPP]
                                    [SLIP]
                                    [INTERACTIVE]
```

Where	Means
LOGOUT	Log off the port if APD is unable to determine which protocol is being used to make the connection. This is the default.
ARAP	Select ARAP as the protocol to use for a connection if APD is unable to determine which protocol is being used to make the connection.
PPP	Select PPP as the protocol to use for a connection if APD is unable to determine which protocol is being used to make the connection.
SLIP	Select SLIP/CSLIP as the protocol to use for a connection if APD is unable to determine which protocol is being used to make the connection.
INTERACTIVE	Permit only an interactive connection if APD is unable to determine which protocol is being used to make the connection.

Example

```
DEFINE PORT 6-12 APD DEFAULT PPP
```

DEFINE PORT APD PROMPT

Use this command to define whether or not the APD prompt will be displayed on a specific port.

Syntax

```
DEFINE PORT <port-list> APD PROMPT [ENABLED]
                                   [DISABLED]
```

Where	Means
ENABLED	The APD prompt will be displayed on the specified port(s). The default prompt is “AUTOMATIC PROTOCOL DETECTION - Begin Protocol or enter 4 returns for interactive mode.”.
DISABLED	No prompt will be displayed.

Example

```
SET PORT 20 APD PROMPT ENABLED
```

DEFINE/SET PORT APD TIMEOUT Privilege: P

Use this command to specify how much time an APD port can spend attempting to determine which protocol is being used to make a connection.

Access server ports can be configured to accept connections made via different protocols, using the Automatic Protocol Detection (APD) feature. Using APD, ports will automatically determine the protocol being used to make a connection and adjust port settings appropriately. Alternatively, by not enabling APD, ports can be dedicated for use by a single access serving protocol. An individual port can be configured to accept any connections made via ARAP, PPP, SLIP (which includes CSLIP), and interactive protocols, as well as all or none of these.

Syntax

```
DEFINE PORT port-list APD TIMEOUT [time]
                                  [UNLIMITED}
```

Where	Means
time	Specifies how much time the port can spend in an attempt to determine which protocol is being used to make a connection. Valid timeout values are from 1 to 255 seconds.
UNLIMITED	The port can continue indefinitely trying to determine which protocol is being used to make a connection.

Example

```
DEFINE PORT 6-12 APD TIMEOUT 30
```

DEFINE PORT ARAP Privilege: P

The AppleTalk Remote Access Protocol (ARAP) lets a Macintosh user connect to an AppleTalk network through a Xyplex access server. The server transfers AppleTalk packets between the remote Macintosh and the AppleTalk network in such a way that the Macintosh acts as if it were directly connected to the network.

Use this command to specify whether or not ARAP can be used on a given port. When ARAP is enabled on a port, interactive sessions and other protocols will not be available on the port (i.e., the port is dedicated only to Remote Access connections). The ARAP protocol must be enabled on the server in order to enable Remote Access (ARAP) at one or more ports. See the DEFINE/SET SERVER PROTOCOL ARAP command for more information.

The unit will verify that certain port settings are set properly before enabling Remote Access on the port. These settings are:

Characteristic	**Setting**
PORT ACCESS	LOCAL
PORT FLOW CONTROL	CTS or NONE (depending on configuration)
PORT MODEM CONTROL	DISABLED
PORT AUTOBAUD	DISABLED

There is no SET command for enabling or disabling Remote Access on a port.

See the Using TCP/IP Features section of the *Advanced Configuration Guide* for more information about setting up Remote Access on the access server.

Syntax

```
DEFINE PORT [port-list] ARAP  [ENABLED]
                              [DISABLED]
```

Where	**Means**
port-list	One or more ports where you want to specify the status of the Remote Access feature (ARAP).
ENABLED	The Remote Access feature (ARAP) can be used on this port.
DISABLED	The Remote Access feature (ARAP) cannot be used on this port. This is the default.

Example

Use the following command to enable ARAP at ports 1 through 5:

```
DEFINE PORT 1-5 ARAP ENABLED
```

DEFINE PORT ARAP GUEST LOGINS ENABLED/DISABLED Privilege: P

Use this command to specify whether or not users can login to the Remote Access server as a guest.

When a user connects to the network via Remote Access, the Remote Access login window includes an option to allow users to log on to the device as a "guest" user (no password is required to log in as a guest user), rather than as a "registered" user. Administrators of AppleTalk Remote Access servers can control whether or not guest logins are permitted on one or more ports.

Note: *There is no SET command for enabling or disabling guest access on a port. See Using the TCP/IP Features in the* Advanced ConfigurationGuide *for more information.*

Syntax

```
DEFINE PORT [port-list] ARAP GUEST LOGINS [ENABLED]
                                          [DISABLED]
```

Where	Means
port-list	One or more ports where guest logins will be enabled or disabled.
ENABLED	A user at this port can login as a guest user.
DISABLED	A user at this port cannot login as a guest user. This is the default.

Example

```
DEFINE PORT 1-5 ARAP GUEST LOGINS ENABLED
```

DEFINE PORT ARAP MAXIMUM CONNECT TIME Privilege: P

Use this command to specify a connection time limit. The server manager can configure a port so that ARAP users have a limited amount of time in which to remain connected. When the ARAP session reaches the limit, the server will disconnect the session.

Note: *There is no SET command to change this value temporarily on a port. See Using the TCP/IP Features section of the* Advanced Configuration Guide *for more information.*

Syntax

```
DEFINE PORT [port-list] ARAP MAXIMUM CONNECT TIME  [time]
                                                   [UNLIMITED]
```

Where	Means
port-list	One or more ports where you want to specify maximum connection time.
time	Users at this port can connect for the specified amount of time (in minutes).
UNLIMITED	Users at this port can connect for an indefinite amount of time. This is the default.

Example

```
DEFINE PORT 1-5 ARAP MAXIMUM CONNECT TIME 30
```

SET PORT ARAP TIME REMAINING — Privilege: P

Use this command for one or more ports, while there are active Remote Access sessions. This command changes the amount of time the user has available for the session. The user of the session will be notified that the server manager has changed the time remaining for the current session, and how much time remains. This gives users an opportunity to finish whatever they are doing and log out the port. The next time a user logs on to the port, that user will be allowed to remain connected for the period of time specified by the PORT ARAP MAXIMUM CONNECT TIME setting.

Notes: *You do not need to use this command prior to reinitializing the server, in order to notify users that the server will be reinitializing. When you use the INITIALIZE DELAY command, and time is greater than 1 minute, the server notifies all logged in ports.*

There is no DEFINE command for changing this value.

Syntax

```
SET PORT [port-list] ARAP TIME REMAINING     [UNLIMITED]
                                             [NONE]
                                             [time]
```

Where	Means
port-list	One or more ports where you want to specify the ARAP time remaining value.
UNLIMITED	Users at this port can stay connected for an indefinite amount of time.
NONE	Users at this port will be disconnected immediately (i.e., they have no more time).
time	Users at this port can stay connected only for the specified amount of time (in minutes). The user will be notified of the change.

Example

```
DEFINE PORT 1-5 ARAP TIME REMAINING 5
```

DEFINE PORT ARAP ZONE ACCESS Privilege: P

Use this command to specify which AppleTalk zones are available to users at a specific port. This command can be used to restrict remote access to devices in one or more AppleTalk zones.

All AppleTalk devices are found in an AppleTalk zone, which can be an EtherTalk zone, a TokenTalk zone, a LocalTalk zone, etc. There is always a default choice for the zone which the device will join. Xyplex access servers join an EtherTalk zone. The user can select Chooser entities (printers, file servers, Public Folders, or other peripheral devices) located in other zones.

Note: *There is no SET command for changing the ARAP zone access on a port.*

Syntax

```
DEFINE PORT [port-list] ARAP ZONE ACCESS  [ALL]
                                          "zone-name"
                                          [LOCAL]
                                          [NONE]
```

Where	Means
port-list	One or more ports where you want to specify the zone access.
ALL	Users at this port have access to all AppleTalk zones. This is the default.
LOCAL	Users at this port have access only to the AppleTalk zone that the server is in.
NONE	Users at this port do not have access to AppleTalk zones. While users cannot see services on the network, they can still provide services to others.
"zone-name"	Users at this port have access to the specific AppleTalk zone specified by the zone-name, in addition to the zone that the server is in. A zone-name is a quoted text string that can be up to 32 characters in length and cannot contain the double-quote (") character.

Example

```
DEFINE PORT 1-5 ARAP ZONE ACCESS NONE
```

DEFINE/SET PORT AUTHORIZED GROUPS Privilege: P

Use this command to set or change the groups to which the specified port(s) or all ports are authorized to have LAT access. Each device (service node, access server, etc) in a LAT network is assigned one or more group codes (this includes devices that offer services and those that do not offer services). At periodic intervals, each device that offers a service to the network broadcasts an announcement to indicate that the service is available and which group codes may have access to the service. Thus, the server manager can permit (authorize) or restrict access to services by selecting which group codes are enabled or disabled for various ports.

See the Using the TCP/IP Features section of the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE/SET PORT port-list AUTHORIZED GROUPS [group-list]
                                            [DISABLED]
                                            [ENABLED]
```

Where	Means
group-list	Valid values for group-lists are 0 to 255. You can specify multiple groups in a group-list by specifying individual group numbers separated by commas, by specifying a range of group-numbers separated by a hyphen, or a combination of both (do not include spaces). For example, the group-list: 1,23-25,48 refers to the individual groups: 1, 23, 24, 25, and 48. When you specify a group-list, without specifying the ENABLED or DISABLED keyword (see below), the specified group-list replaces the current list for the port(s). The default authorized groups are: 0 ENABLED and 1 through 255 DISABLED.
DISABLED	The authorized groups, listed in the group-list, are removed from the list of groups available to the specified port(s) or all ports on the server.
ENABLED	Specifies that authorized groups, listed in the group-list, are added to the list of groups available to the specified port(s) or all ports on the server.

Example

```
DEFINE PORT 5 AUTHORIZED GROUPS 3-12,15 ENABLED
```

DEFINE/SET PORT AUTOBAUD Privilege: P

Use the PORT AUTOBAUD command to specify whether or not the port will determine the input port speed, parity, and character size for the device connected to the port, and automatically set the matching server port settings. The server uses the ASCII RETURN character to determine the port speed, parity, and character size. Normally, the user must press the RETURN key a few times until the server determines the port speed, parity, and character size, and begins a logon sequence. This command does not apply to parallel ports.

You can only enable AUTOBAUD where the attached device is configured with the following settings at a port set to LOCAL ACCESS and:

CHARACTER SIZE	8, (7 if EVEN parity)
PARITY	NONE (EVEN if character size is set to 7)
SPEED	Valid speeds between 50 and 38400 as listed below.

The supported port speeds are: 50, 75, 110, 134, 150, 300, 600, 1200, 1800, 2000, 2400, 4800, 9600, 14400, 19200, 21600, 26400, 28800, 33600, and 38400 bits per second (baud). The device connected to the port must be set to one of these speeds. (Ports cannot autobaud at port speeds above 38400 bps.

Note: *Access servers do not autobaud when the port receives 7-bit characters with EVEN parity from the device until software loading has completed. You must use 8-bit characters with parity set to NONE in order to receive load messages and to enter into the ROM Configuration Menu.*

Syntax

```
DEFINE/SET PORT [port-list] AUTOBAUD      [DISABLED]
                                          [ENABLED]
```

Where	Means
DISABLED	The port will not determine the port speed, parity, and character size at port login, and will not automatically set matching terminal port characteristics. Any connecting device will operate at the settings stored in the permanent database.
ENABLED	The port will determine port speed, parity, and character size at port login, and will automatically set these matching port characteristics. This is the default setting.

Example

```
DEFINE PORT 5 AUTOBAUD DISABLED
```

DEFINE/SET PORT AUTOCONNECT Privilege: S, N, P

Use this command to specify whether or not the port will automatically connect to either a dedicated service or a preferred service when the user logs on to a port. Autoconnect is automatically enabled for a port when a dedicated or preferred service is defined for that port. However, it is not disabled when service is disabled.

Autoconnect also specifies whether or not the port should attempt to re-connect a session when a connection failure occurs. Re-connection attempts occur at intervals specified by the SERVER KEEPALIVE TIMER command (between 10 and 180 seconds), and a status message displays whenever ports that are not configured with a dedicated service attempt to connect (no messages are given for ports that are configured with a dedicated service). Re-connection attempts continue until a connection is made or the user terminates further attempts by entering the local command mode.

Finally, Autoconnect helps control server activity when the port uses modem control signals (for example, a port connected to a dial-up line). Before you can enable Autoconnect, you must define the port for LOCAL access, enable MODEM CONTROL, and define a dedicated service.

Syntax

```
DEFINE/SET PORT port-list AUTOCONNECT  [ENABLED]
                                       [DISABLED]
```

Where	Means
ENABLED	The port will automatically connect to a dedicated or preferred service when the port is logged on, and it will automatically attempt to re-connect a session when a connection failure occurs; the server will not log out the port when a session ends.
DISABLED	The server will not automatically connect to a service when the port is logged on; the server will log out the port when a session ends or a connection failure occurs. This is the default.

Example

```
DEFINE PORT 5 AUTOCONNECT ENABLED
```

DEFINE/SET PORT AUTODEDICATED Privilege: P

The AUTODEDICATED command specifies whether or not the unit will automatically log on the port and establish a connection to the dedicated service that is defined for the port (via the PORT DEDICATED SERVICE, LAT DEDICATED SERVICE, or TELNET DEDICATED SERVICE command) when the unit is initialized or the port is logged out. The auto-dedicated command causes the unit to bypass the login routine and connect the port directly to the dedicated service. If you log out the port, the unit logs on the port again and re-connects to the dedicated service.) Use the AUTODEDICATED command for ports that are connected to devices that are unable to send a character (such as a CR/LF) to initiate a session.

Note: *If PORT AUTOBAUD is ENABLED, the unit waits until the port is autobauded before the connection is made.*

Syntax

```
DEFINE/SET PORT [port-list] AUTODEDICATED[ENABLED]
                                         [DISABLED]
```

Where	Means
ENABLED	The unit will automatically log on the port and establish a connection to the specified dedicated service when the unit is initialized or the port is logged out.
DISABLED	The unit will not automatically log on the port when the unit is initialized or the port is logged out. This is the default.

Example

```
DEFINE PORT 5 AUTODEDICATED ENABLED
```

DEFINE/SET PORT AUTOHANGUP Privilege: P

Use this command to automatically log out of a port after the last session is terminated.

Syntax

```
DEFINE/SET PORT <port-list> AUTOHANGUP [ENABLED]
                                       [DISABLED]
```

Where	Means
port-list	One or more ports where you want to enable/disable autohangup.
ENABLED	The specified ports will automatically log out when the last session is terminated.
DISABLED	The specified ports will not be logged out when the last session is terminated. This is the default setting.

Example

```
DEFINE PORT 6,8,9 AUTOHANGUP ENABLED
```

DEFINE/SET PORT AUTOPROMPT Privilege: S

Use this command to specify whether or not the port will automatically prompt the service node to initiate a system-specific login sequence (i.e., have the service node run its login routine) when a port connection is made. The service node must support this setting. This setting only applies to LAT sessions.

Syntax

```
DEFINE/SET PORT port-list AUTOPROMPT   [DISABLED]
                                      [ENABLED]
```

Where	Means
DISABLED	The server will not prompt the service node to initiate its login sequence. In this case, the user must initiate a login sequence (for example, by pressing the RETURN key).
ENABLED	The server will prompt the service node to initiate its login sequence. This is the default setting.

Example

```
DEFINE PORT 5 AUTOPROMPT ENABLED
```

DEFINE/SET PORT BACKWARD SWITCH Privilege: S, N, P

Use this command to specify whether or not there will be a character which when entered, that allows a user to return to the previous (lower-numbered) session, without returning to the local command mode.

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT [port-list] BACKWARD SWITCH [character]
                                           [NONE]
```

Where	Means
character	A keyboard character that the user will type to return to the previous session. It is recommended that you specify an unused CTRL character. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, or with the character you set for the FORWARD SWITCH, the LOCAL SWITCH, or any Telnet command characters). If you do specify a CTRL character, when the user types the character, it will be displayed as ^<Key> (i.e., if the user types CTRL/B, the terminal will echo the characters: ^B).
NONE	The user cannot type a character to return to the previous session (therefore, the user will need to return to the local command mode in order to return to the previous session). This command can be used to remove a previously defined backward switch character. This is the default setting.

Example

```
DEFINE PORT 5 BACKWARD SWITCH ^B
```

DEFINE/SET PORT BREAK Privilege: N

Use this command to specify the action that the port will take when the user presses the BREAK key.

If you send a break during a Telnet session to a port whose PORT BREAK is set to REMOTE, you may observe unexpected behavior (for example, bad output). The server will send a break signal to the connection partner for the time length specified by the DEFINE PORT BREAK LENGTH setting.

This command does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list BREAK  [LOCAL]
                                 [REMOTE]
                                 [DISABLED]
```

Where	Means
DISABLED	The server will ignore the BREAK key.
LOCAL	The server will return to the local command mode when the user presses the BREAK key. This is the default setting.
REMOTE	The server will send the break to the connection partner, when the user presses the BREAK key.

Note: *In a Telnet session, if you want to use the BREAK key to generate the Telnet Attention character, set the BREAK to REMOTE.*

Example

```
DEFINE PORT 5 BREAK LOCAL
```

DEFINE/SET PORT BREAK LENGTH Privilege: P

Use this command to specify the time length of a break sent out of the serial port in response to a TELNET BREAK.

Notes: *This command does not work under LAT. BREAK MUST be set on the port for this option to work.*

When a break time length is defined, the following events occur:

- TELNET sends a TELNET Break over the network to the Access Server.
- The TELNET Break is received and the port's line driver chip is signaled to transmit a break out over the serial line.

Notes: *This command will not work if the DEFAULT SESSION MODE is set to TRANSPARENT or INTERACTIVE_NOIAC.*

Use the SHOW/LIST PORT CHARACTERISTICS command to display the current break length setting.

Syntax

```
DEFINE PORT <port number> BREAK LENGTH <time-length>
```

Where	Means
port number	The port number that will be set for the break time length.
time-length	This value can be one of the following:
	MS_250 indicates a break of 250 milliseconds. This is the default.
	MS_500 indicates a break of 500 milliseconds
	MS_750 indicates a break of 750 milliseconds

Example

```
DEFINE PORT 6 BREAK LENGTH MS_750
```

DEFINE/SET PORT BROADCAST Privilege: N, P

Use this command to specify whether or not this port will display messages that are broadcast from other ports on this server.

Typically, you would permanently disable the display of messages for ports which are connected to devices such as printers, or temporarily disable the display of messages when you do not want to be disturbed by broadcasted messages.

Syntax

```
DEFINE/SET PORT port-list BROADCAST [DISABLED]
                                   [ENABLED]
```

Where	Means
DISABLED	Specifies that this port will not display messages that are broadcast from other ports on this server.
ENABLED	Specifies that this port will display messages that are broadcast from other ports on this server. This is the default.

Example

```
DEFINE PORT 5 BROADCAST DISABLED
```

DEFINE/SET PORT CCL MODEM AUDIBLE/INAUDIBLE Privilege: P

You can configure a port so it indicates to the CCL script whether or not the modem speaker should be audible while the modem establishes a connection. Whether or not the modem speaker is audible has no effect on CCL script execution.

Syntax

```
DEFINE/SET PORT [port-list] CCL MODEM     [AUDIBLE]
                                          [INAUDIBLE]
```

Where	Means
port-list	One or more ports where you want to change this CCL modem setting.
AUDIBLE	Indicate to the CCL script that the modem should be audible while the modem establishes the connection.
INAUDIBLE	Indicate to the CCL script that the modem should not be audible while the modem establishes the connection. This is the default.

Example

```
DEFINE PORT 1-5 CCL MODEM INAUDIBLE
```

DEFINE PORT CCL NAME Privilege: P

CCL scripts are ASCII text files which contain commands that specify initialization and operational characteristics for the specific type of modem that is connected to a port. CCL scripts are stored at script servers (hosts which can transfer a file to the server via TFTP) and usually indicate the type of modem connected to the port. Individual ports can be configured to use a specific CCL script using the DEFINE PORT CCL NAME command.

To configure a script server, the correct location (directory path and name) for the ccl-script-file is required, and should be as follows:

```
directory-path/CCL/ccl-name
```

Where	Means
`directory-path`	The directory on the script server where scripts are stored. Use the DEFINE SERVER SCRIPT SERVER command to specify the directory-path. The directory path is usually the TFTP home directory on a UNIX host.
`CCL`	The scripts are contained in a /CCL sub-directory of the `directory-path`.
`ccl-name`	A file name which usually indicates the type of modem connected to the port.

All space characters are removed from the name before it is concatenated with the directory path. The '/' characters above indicate where the separator character will be inserted in the path.

If no CCL script is specified on the port, the server manager must manually configure the port and modem for proper Remote Access operation. Use this setting for ports where ARAP (AppleTalk Remote Access Protocol) is enabled.

Xyplex supplies CCL scripts for use with a variety of modems. These are listed in the Scripts section of the *Advanced Configuration Guide.*

Note: *There is no SET command for specifying CCL script server names.*

Syntax

```
DEFINE PORT [port-list] CCL NAME    ["ccl-script-file"]
                                    [NONE]
```

DEFINE PORT CCL NAME (continued)

Where	Means
port-list	One or more ports where you want to specify a CCL script name.
"*ccl-script-file*"	The name of a CCL script, which is located in a /CCL sub-directory at a script server.
NONE	The port will not be a assigned CCL script. This is the default.

Example

```
DEFINE PORT 1-5 CCL NAME "Telebit_T3000"
```

DEFINE/SET PORT CHARACTER SIZE Privilege: N

Use this command to specify the number of bits per character for data characters that are transmitted/received over the server serial interface (e.g., between the server and the device connected to the port).

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT [port-list] CHARACTER SIZE[5]
                                          [6]
                                          [7]
                                          [8]
```

Where	Means
5	The port serial interface transmits/receives data characters using a five bits per character format.
6	The port serial interface transmits/receives data characters using a six bits per character format.
7	The port serial interface transmits/receives data characters using a seven bits per character format.
8	The port serial interface transmits/receives data characters using an eight bits per character format. This is the default.

Example

```
DEFINE PORT 5 CHARACTER SIZE 7
```

DEFINE/SET PORT CLEAR IP SECURITY ENTRIES Privilege: P

Use this command to clear entries the Internet Security table when modem signals are deasserted at a port or a connection is disconnected. This feature is useful when many users log in to a unit whose ports are configured to use login scripts containing commands that configure Internet security entries.

Internet security allows you to permit or restrict inbound and outbound connection requests on an Internet network. You can permit/restrict outbound connections from specific ports to specific Internet addresses and to particular nodes at an Internet address. You can permit/restrict inbound connections to specific ports from specific Internet addresses and particular nodes at an Internet address.

See the Security Features section of the *Advanced Configuration Guide* for more information on Internet Security.

Syntax

```
DEFINE/SET PORT port-list CLEAR IP SECURITY ENTRIES      [ENABLED]
                                                            [DISABLED]
```

Where	Means
ENABLED	The Internet security table will be cleared when modem signals are deasserted at a port or a connection is disconnected.
DISABLED	The Internet security table will not be cleared when modem signals are deasserted at a port or a connection is disconnected. This is the default.

Example

```
DEFINE PORT 6 CLEAR IP SECURITY ENTRIES ENABLED
```

DEFINE PORT COMMAND SIZE Privilege: P

Use this command to control the size of the command input buffer. Use the SHOW PORT ALTERNATE CHARACTERISTICS command to display the current size.

Note: *This setting cannot be modified by a SET command.*

Syntax

```
DEFINE PORT [port-list] COMMAND SIZE [size]
```

Where	Means
port-list	The ports where you want to change the command size buffer.
size	The size of the command input buffer. Valid values are from 80 to 16384. The default setting is 80.

Example

```
DEFINE PORT COMMAND SIZE 1000
```

DEFINE/SET PORT CONNECTRESUME Privilege: N

Use this command to specify how the port will handle a connection attempt (e.g., a CONNECT command) to a destination when a session with that destination already exists. Depending on the setting for this option, the CONNECT command can either establish a new session to the destination, or resume an existing session with the destination.

Syntax

```
DEFINE/SET PORT port-list CONNECTRESUME   [DISABLED]
                                          [ENABLED]
```

Where	Means
DISABLED	The port will allow the CONNECT command to establish a new session to a destination, rather than resume an existing session with the destination. This is the default setting.
ENABLED	The port will allow the CONNECT command to resume an existing session with the specified destination, rather than establishing a new session to that destination.

Example

```
DEFINE PORT 5 CONNECTRESUME ENABLED
```

DEFINE/SET PORT CONTROLLED PORT Privilege: P

Use this command to specify the string(s) sent to the console during port logout or login. You can use these strings to change the settings on the terminal when you log into or out of a port.

The strings are hexadecimal ASCII characters, enclosed in double quotes, with each byte separated by a space, such as "0d 0a"

The default string is the null string; a pair of double quotes(""). To clear a string, set it to the null string "".

Syntax

```
DEFINE/SET PORT port-list CONTROLLED PORT [LOGIN "string"]
                                          [LOGOUT "string"]
```

Where	Means
LOGIN	When logging into a port, send the following ASCII hexadecimal sequence "*string*" out the port to the terminal.
LOGOUT	When logging out of a port, send the following ASCII hexadecimal sequence "*string*" out the port to the terminal.
"*string*"	ASCII hexadecimal characters, from 0 to 32, enclosed in double quotes with each byte separated by a space. The default is a null string.

Example

```
DEFINE PORT CONTROLLED PORT LOGIN "1B 5B 48"
```

DEFINE/SET PORT CONTROLLED SESSION Privilege: P

Use this command to specify the string(s) sent to the console during a controlled connection. You can use these strings to change the settings on the terminal when you enter or exit a session during session startup, termination, switching in, or switching out of a session. Note that these strings are only sent out the asynchronous port, and not across the network.

Syntax

```
DEFINE/SET PORT CONTROLLED SESSION [INITIALIZE "string"]
                                   [TERMINATE "string"]
```

Where	Means
INITIALIZE	When starting, resuming, or switching to a session, send the following *"string"* to the console.
TERMINATE	When ending or switching out of a session, send the following *"string"* to the console.
"*string*"	ASCII hexadecimal characters, from 0 to 32, enclosed in double quotes with each bytes separated by a space. The default string is the null string (a pair of double quotes""). To clear a string, set it to the null string "".

Example

```
DEFINE PORT CONTROLLED SESSION INITIALIZE "07"
```

DEFINE/SET PORT DCD TIMEOUT Privilege: P

Use this command to set or change the period of time that the DCD signal can be deasserted, before the software will disconnect the port. The value you set does not affect the requirement that the DCD signal be asserted by the device for at least two seconds, before modem control "handshaking" is considered to be established. This command requires that you enable MODEM CONTROL.

This command does not apply to parallel ports or serial ports that do not support modem control signals.

Syntax

`DEFINE/SET PORT [`*`port-list`*`] DCD TIMEOUT [`*`timer-value`*`]`

Where	Means
timer-value	The period of time that the DCD signal can be deasserted before the software will disconnect the port. The range for this variable is between 0 and 10000 milliseconds in increments of 100 milliseconds. Setting this value to 0 means that the port will deassert the DTR signal immediately after DCD is deasserted. The default value is 2000 milliseconds (2 seconds).

Example

```
DEFINE PORT 5 DCD TIMEOUT 2000
```

DEFINE PORT DEDICATED SERVICE Privilege: P

Use this command to specify whether or not there will be a service to which the port is permanently assigned, or that there will be a change made to the current permanent service assignment for the port. This command automatically connects the port to a dedicated service, whenever a user logs on to that port.

When a connection is attempted, the server interprets the variable which follows this keyword as either a LAT *service-name* or as a Telnet destination (*domain-name* or *internet-address*), depending on the RESOLVE SERVICE setting. You can also specify the prefixes LAT or TELNET to require the server to interpret the variable as a LAT *service-name* or a Telnet destination. (See the descriptions of the RESOLVE SERVICE, LAT DEDICATED SERVICE and TELNET DEDICATED SERVICE commands and the Dedicated Service section in the *Advanced Configuration Guide* for more information.)

Note: *You can only use a DEFINE command to specify the PORT DEDICATED SERVICE. There is no SET command.*

Syntax

```
DEFINE PORT port-list  DEDICATED SERVICE service-information
```

where the following is the syntax for *service-information*:

```
[service-name] [NODE] [node name]       [DESTINATION][port name] [CONTROLLED]
                                                     [NONE]
                      [NONE]            [DESTINATION][port name]
                                                     [NONE]
               [NONE] [NODE]            [node name]  [DESTINATION][port name]
                                                     [NONE]
                      [NONE]                   [DESTINATION][port name]
                                                     [NONE]
               [domain-name[:telnet-port number]]
               [internet-address[:telnet-port number]]
```

DEFINE PORT DEDICATED SERVICE (continued)

Where	Means
service-name	The name of a LAT service to which the port is permanently assigned.
NODE	Specifies that you will set or change the name of the service node on which the dedicated service is offered. (This keyword only applies to services that are offered on a LAT network.)
node name	The name of the service node at which the dedicated service is offered.
DESTINATION	Specifies that you will set or change the name of the server port at which the dedicated service is offered. (This keyword only applies to services that are offered on a LAT network.)
port name	The name of the server port where the service, specified by the service-name, is offered.
NONE	Specifies that this port, all ports, or the ports listed in the port-list will not have a dedicated service, or that you wish to cancel a previously defined dedicated service, service node, or destination server port setting. This is the default setting.
domain-name	The logical name of the Telnet destination to which the port is permanently assigned. If the specified domain-name is not a fully qualified domain-name, the specified name will be concatenated with the default Internet domain-name-suffix.
internet-address	The identity or location of the Telnet destination on the network where the port is permanently assigned.
:*telnet-port number*	The number of the target Internet protocol or physical port address which will be used for sessions between the port and the Telnet destination to which the port is permanently assigned. Note that the colon character (:) is required to separate the telnet-port number from the domain-name.
CONTROLLED	Causes the connection to use the strings defined by the DEFINE/SET PORT CONTROLLED SESSION command.

Example

```
DEFINE PORT 5 DEDICATED SERVICE FINANCEVAX
```

DEFINE/SET PORT DEFAULT SESSION MODE Privilege: P

Use this command to specify the initial setting for all sessions.

After an outbound Telnet session is formed from the server, if the remote partner attempts to negotiate the Telnet binary option, the server will use the value set for the PORT TELNET BINARY SESSION MODE to determine session mode.

When binary option negotiation is initiated from a remote host for an inbound Telnet session, the server will use the PORT TELNET BINARY SESSION MODE setting to determine what mode to use for the session.

If you establish a Telnet session without specifying binary mode, the session defaults to interactive mode, regardless of the default port session mode setting.

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list DEFAULT SESSION MODE     [INTERACTIVE]
                                                   [INTERACTIVE_NOIAC]
                                                   [PASTHRU]
                                                   [PASSALL]
                                                   [TRANSPARENT]
```

DEFINE/SET PORT DEFAULT SESSION MODE (continued)

Where	Means
INTERACTIVE	The server initially sets all sessions so that all switching characters, Telnet command characters, and XON/XOFF flow control recognition are enabled, and will not negotiate the Telnet binary option. This is the default.
INTERACTIVE _NOIAC	The server initially sets all sessions so that a Telnet session ignores Telnet option messages received from a remotely initiated session and does not send any Telnet option messages from the locally initiated session, in addition to disabling all switching characters, and Telnet command characters. For example, if an FF (hex 255) is received from the network, this character is inserted into the output console ring to be delivered to the serial port and likewise for the character following. The exception to this is if an FF follows an FF, the second FF is discarded and not inserted into the output console ring.
PASTHRU	The server will initially set all sessions so that all switching characters and Telnet command characters are interpreted as data, and will negotiate the Telnet binary option. Note that XON/XOFF flow control can still be used in this mode.
PASSALL	The server will initially set all sessions so that all switching characters, Telnet command characters, and XON/XOFF flow control recognition are disabled, and will negotiate the Telnet binary option. Use this mode whenever full data transparency is required, but option negotiations are to be recognized.
TRANSPARENT	The server will initially set all sessions so that a Telnet session will ignore Telnet option messages received from a remotely initiated session and will not send any Telnet option messages from the locally initiated session, in addition to disabling all switching characters, and Telnet command characters. For a LAT session, the server tells its partner it is PASSALL but acts locally as if it were PASTHRU. Transparent is invalid for LAT sessions whose PORT ACCESS is REMOTE or DYNAMIC. Use this mode whenever full data transparency is required, but no option negotiations are to be recognized.

Example

```
DEFINE PORT 5 DEFAULT SESSION MODE PASSALL
```

DEFINE/SET PORT DIALBACK Privilege: P

Use this command to specify whether or not the port requires a dialback script in order to be logged in. The dialback script contains commands that cause a modem to dial a designated telephone number.

Note: *Before you can use the dialback feature, enable modem control on the port. Use the DEFINE/SET PORT MODEM CONTROL command to do this. To check the current modem control setting, use the SHOW PORT CHARACTERISTICS command. The default for modem control is disabled.*

Syntax

```
DEFINE/SET PORT port-list DIALBACK  [DISABLED]
                                    [ENABLED]
                                    [TIMEOUT time]
```

Where	Means
DISABLED	The port does not require a dialback script in order to be logged in. This is the default.
ENABLED	The port requires a dialback script in order to be logged in.

Example

```
DEFINE PORT 5 DIALBACK ENABLED
```

DEFINE/SET PORT DIALBACK TIMEOUT Privilege: P

Use this command to specify whether or not the port will have only a specified amount of time to answer a dialback call.

Syntax

```
DEFINE/SET PORT [port-list] DIAL BACK TIMEOUT [seconds]
```

Where	Means
TIMEOUT	The amount of time that the remote modem (the modem being called) has to answer a dialback call.
time	The amount of time that the remote modem (the modem being called) has to answer a dialback call. The range for this variable is between 5 and 60 seconds (do not specify units). The default value is 20 seconds.

Example

```
DEFINE PORT 5 DIALBACK TIMEOUT 10
```

DEFINE/SET PORT DIALOUT ACTION Privilege: P

Use this command to designate what action the port should take when the remote session made at a dial-out port is terminated by the connection partner. This is useful for setting up a link so that it provides a limited dialout routing capability for connecting two LANs (i.e., a PPP or SLIP gateway).

Syntax

```
DEFINE/SET PORT [port-list] DIALOUT ACTION  [PPP]
                                            [SLIP]
                                            [LOGOUT]
                                            [QUERY]
```

Where	Means
PPP	After terminating the remote session, the port will go from "interactive" to PPP mode.
SLIP	After terminating the remote session, the port will go from "interactive" to SLIP mode.
LOGOUT	Disconnect the link and logout the port. This is the default.

QUERY	Ask the user which of the above actions the port should take. When QUERY is selected, after the remote connection is established, the user is prompted with the following question:
	
	`Please select a logout option from the following choices:`
	
	`PPP, SLIP, or LOGOUT:`
	
	The user selects PPP, SLIP, or LOGOUT (the meanings are the same as for the DEFINE/SET PORT DIALOUT ACTION command) and presses the RETURN key. If the user simply presses the RETURN key, or specifies an invalid selection three consecutive times, the unit selects the LOGOUT option automatically.

Example

```
DEFINE PORT 5 DIALOUT ACTION PPP
```

DEFINE/SET PORT DIALUP — Privilege: P

Use this command to specify to LAT service nodes whether or not the port is connected to a dial-up line. When a service node receives a connection request, the node will accept or reject the request based on the DIALUP setting.

Syntax

```
DEFINE/SET PORT port-list DIALUP     [DISABLED]
                                     [ENABLED]
```

Where	Means
DISABLED	The port is not connected to a dial-up line. This is the default setting.
ENABLED	The port is connected to a dial-up line.

Example

```
DEFINE PORT 5 DIALUP ENABLED
```

DEFINE/SET PORT DISCARD ERRORS Privilege: P

Use this command to set up the serial controller on the specified port to discard characters received in error without notifying the software.

Syntax

```
DEFINE PORT <port-list> DISCARD ERRORS [ENABLED]

                                       [DISABLED]
```

Where	Means
ENABLED	If enabled, characters received in error on the specified ports will be discarded without notifying the software
DISABLED	Characters received in error on the specified port will not be discarded.

DEFINE/SET PORT DSRLOGOUT Privilege: P

Use this command to specify whether or not the server should log out a port when the DSR signal is deasserted. The DSRLOGOUT keyword only applies for ports where the MODEM CONTROL is DISABLED.

Do not use DSRLOGOUT if the port is used for TN3279 print screens (see the DEFINE/SET PORT ACCESS PRT3270 command).

See Setting up Basic Modem Applications in the *Basic Configuration Guide* for more information.

This command does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT [port-list] DSRLOGOUT  [DISABLED]
                                       [ENABLED]
```

Where	Means
DISABLED	Do not log out the port when the serial interface DSR signal is lost. This is the default setting.
ENABLED	Logout the port when the serial interface DSR signal is lost.

Example

```
DEFINE PORT 5 DSRLOGOUT ENABLED
```

DEFINE/SET PORT DSRWAIT Privilege: P

Use this command to specify whether or not the server should begin the login sequence when the device asserts the DSR signal.

See Setting up Basic Modem Applications in the *Basic Configuration Guide* for more information.

This command does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT [port-list] DSRWAIT [DISABLED]
                                    [ENABLED]
```

Where	Means
DISABLED	The server should not begin the login sequence when the device asserts the DSR signal. This is the default setting.
ENABLED	The server should begin the login sequence when the device asserts the DSR signal. This setting requires that ACCESS be set to LOCAL or DYNAMIC and MODEM CONTROL be set to ENABLED.

Example

```
DEFINE PORT 5 DSRWAIT ENABLED
```

DEFINE/SET PORT DTRWAIT Privilege: P

Use this command to determine when the server port should assert the DTR modem control signal line. You must also enable MODEM CONTROL. This command does not apply to parallel ports.

See Setting up Basic Modem Applications in the *Basic Configuration Guide* for more information.

Syntax

```
DEFINE/SET PORT port-list DTRWAIT   [DISABLED]
                                    [ENABLED]
                                    [FORCONNECTION]
                                    [FORRING]
```

Where	Means
DISABLED	The port will continuously assert the DTR signal. This is the default setting. When PORT ACCESS is set to REMOTE and DTRWAIT is set to DISABLED, the server does not wait for the device to assert the DCD signal before accepting data. If PORT ACCESS is set to DYNAMIC and DTRWAIT set to DISABLED, assertion of the DCD signal by the device will cause the port to accept local connections only. (In some prior releases, this was an invalid combination of PORT settings.)
ENABLED	The port will assert the DTR signal when a remote connection is made via LAT or Telnet, or when the device connected to the port (e.g., the modem) asserts the RING signal.
FORCONNECTION	The port will assert the DTR signal when a connection is made.
FORRING	The port will assert the DTR signal when the device connected to the port asserts the RING signal.

Example

```
DEFINE PORT 5 DTRWAIT ENABLED
```

DEFINE/SET PORT FLOW CONTROL Privilege: N

Use this command to specify the type of flow control ("handshaking") that is used by the serial interface of the specified port(s). See the *Getting Started Guide* supplied with your unit for a description of associated cabling issues. See the Modems section in the *Basic Configuration Guide* for more information on Flow Control.

This command does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list FLOW CONTROL [CTS]
                                       [DISABLED]
                                       [DSR]
                                       [ENABLED]
                                       [ENQ_HOST]
                                       [ENQ_TERM]
                                       [XON_ALT]
                                       [XON]
```

Where	Means
CTS	The port(s) will use the DCD and DTR modem control signals to provide flow control. (In this case, the DCD and DTR signals are used to emulate RTS/CTS flow control.) This setting is for 6- or 7-wire only. Use CTS/RTS for 8-wire.
DISABLED	The server will not use any flow control methods for the specified port(s).
DSR	The server will use the DCD and DTR modem control signals to provide flow control. (In this case, the DCD and DTR signals are being used to emulate DTR/DSR flow control.)
ENABLED	The server will use flow control for the specified port(s). Uses the last specified setting as the flow control type.
ENQ_HOST	When a host sends an ENQ, the access server port will send an ACL back to the host. Use this setting when a terminal is connected to the port.
ENQ_TERM	Use when an HP host serial port is connected to the access server port.
XON_ALT	The server passes on to the remote end an XON character received from the serial port if the last character sent to the access server was NOT an XOFF.
XON	The server will use XON/XOFF flow control for the specified port(s). This is the default setting.

Example

```
DEFINE PORT 5 FLOW CONTROL CTS
```

DEFINE/SET PORT FORWARD SWITCH Privilege: S

Use this command to specify whether or not a user can switch to the next (higher-numbered) session, without returning to the local command mode.

This command does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list FORWARD SWITCH  [character]
                                          [NONE]
```

Where	Means
character	The keyboard character that the user will type to switch to the next session. Ensure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, or with the character you set for the BACKWARD SWITCH, the LOCAL SWITCH, or any Telnet command characters). If you do specify a CTRL character, when you type the character, it will be displayed as ^<Key> (i.e., if you type CTRL/B, the terminal will echo the characters: ^B).
NONE	There will not be a forwards character, and the user will need to return to the local command mode in order to switch to the next session. Use this command to remove a previously defined forwards character. This is the default setting.

Example

```
DEFINE PORT 5 FORWARD SWITCH ^K
```

DEFINE PORT FROM PORT — Privilege: P

Use this command to copy the permanent characteristics of one port, except the PORT NAME, to one or more other ports on the same unit.

This command can only be used as a DEFINE command.

Syntax

`DEFINE PORT` *`port-list`* `FROM PORT` *`port number`*

Where	Means
port number	The port whose permanent settings, except the PORT NAME setting, are to be copied to the ports specified by the *port-list*.

Example

```
DEFINE PORT 5 FROM PORT 7
```

SET PORT GROUPS — Privilege: N, P

Use this command to specify which LAT services, represented by groups, will be included in server displays shown at your port, the ports listed in the *port-list*, or all ports. Use the SHOW PORT CHARACTERISTICS command to display port settings.

This command is only available as a SET command.

The GROUPS setting permits users to restrict the number of services shown in various server displays. Rather than seeing a lengthy display, users can limit the services shown to those which they use frequently.Note that the groups, listed in this group-list, must be a subset of the groups to which the port is permitted to have access by the AUTHORIZED GROUPS characteristic.

Syntax

```
SET PORT [port-list] GROUPS [group-list]     [DISABLED]
                            [ALL]            [ENABLED]
```

Where	Means
group-list	Valid values for group-lists are between 0 to 255. You can specify multiple groups in a group-list by specifying individual group numbers separated by commas, by specifying a range of group-numbers separated by a hyphen, or a combination of both (do not include spaces). For example, the group-list: 1,23-25,48 refers to the individual groups: 1, 23, 24, 25, and 48. When you specify a group-list, without specifying the ENABLED or DISABLED keyword (see below), the specified group-list replaces the current list for the port(s). The default authorized groups are 0 ENABLED and 1 through 255 DISABLED.
ALL	Specifies that access to all authorized groups will be enabled or disabled. This keyword can be used to cancel the changes to the group list and revert to the list of authorized groups specified by the AUTHORIZED GROUPS characteristic.
DISABLED	The services, represented by the groups listed in the group-list, will not be included in server displays shown at your port, the specified ports, or all ports on the server. However, the port can still connect to these services as long as it is permitted to do so based on the setting of AUTHORIZED GROUPS.

SET PORT GROUPS (continued)

ENABLED — The services, represented by the groups listed in the group-list, will be included in server displays shown at your port, the specified port(s), or all ports on the server. However, the port can only display information about these services as long as it is permitted to do so based on the AUTHORIZED GROUPS setting.

Example

```
SET PORT 5 GROUPS 1,23-25,48 ENABLED
```

DEFINE/SET PORT IDLE TIMEOUT Privilege: P

Use this command to define or change the length of time before an inactive session (for example, a queued connection request or a session initiated by a user) will be disconnected. Ports that have a connection queue, are free to accept the next connection request in the connection queue after the inactive session is disconnected. Typically, this setting is used to prevent a "hung" printer ports, and also to free up access to resources when users forget to logout. This setting applies to Telnet/LAT sessions received by a port on the access server as well as sessions made from the server to a host or other resource out on the LAN.

Ports that do not have a connection queue cause the inactivity timer to start (controlled by the SERVER INACTIVITY TIMER setting) after the sessions have been disconnected. When there have been no sessions at the port, for the period of time specified by the SERVER INACTIVITY TIMER, the user will be logged off the server port.

Syntax

```
DEFINE/SET PORT port-list IDLE TIMEOUT time
```

Where	Means
time	The length of time after which an inactive session will be disconnected. The valid values are between 0 and 480 minutes. Setting this value to 0 disables this setting and the session will not be disconnected for being inactive. The default value is 0.

Example

```
DEFINE PORT 5 IDLE TIMEOUT 10
```

DEFINE/SET PORT INACTIVITY LOGOUT Privilege: P

Use this command to specify whether or not the server will logout a port after a specified period of inactivity. Ports are considered to be inactive while they are in local command mode, do not have any sessions established, and there have been no input, output, or modem signal transitions. The DEFINE/SET SERVER INACTIVITY TIMER command specifies the length of the period of inactivity. See also DEFINE/SET PORT IDLE TIMEOUT for ports that have idle Telnet or LAT sessions.

Syntax

```
DEFINE/SET PORT [port-list] INACTIVITY LOGOUT   [DISABLED]
                                                [ENABLED]
```

Where	Means
DISABLED	The server will not logout a port after a specified period of inactivity has elapsed. This is the default setting.
ENABLED	The server will logout a port after a specified period of inactivity has elapsed.

Example

```
DEFINE PORT 5 INACTIVITY LOGOUT ENABLED
```

DEFINE/SET PORT INPUT FLOW CONTROL Privilege: N

Use this command to specify whether or not flow control will be used for input data communications at the port (i.e., data communication which originates at the device connected to the port and which is received by the server). The flow control method used by the port (e.g., XON/XOFF, DCD/DTR, etc) is specified by the PORT FLOW CONTROL setting.

This command does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT [port-list] INPUT FLOW CONTROL [DISABLED]
                                               [ENABLED]
```

Where	Means
DISABLED	The port will not use flow control for input data communications.
ENABLED	The port will use flow control for input data communications. This is the default setting.

Example

```
DEFINE PORT 5 INPUT FLOW CONTROL ENABLED
```

DEFINE/SET PORT IP CONNECTIONS Privilege: P

Use this command to specify whether or not the port can accept an *internet-address* in order to connect to a TCP/IP destination, or whether all TCP/IP destinations must be specified using the *domain-name* format. This command applies to all connections made via the CONNECT, TELNET CONNECT, RLOGIN, and TELNET CONSOLE commands.

Syntax

```
DEFINE/SET PORT [port-list]  IP CONNECTIONS  [DISABLED]
                                             [ENABLED]
```

Where	Means
DISABLED	The port will not accept an *internet-address* in order to connect to a TCP/IP destination. All TCP/IP destinations must be specified using the *domain-name* format.
ENABLED	The port will accept an *internet-address*, as well as addresses using the *domain-name* format, in order to connect to a TCP/IP destination. This is the default setting.

Example

```
DEFINE PORT 5 IP CONNECTIONS ENABLED
```

DEFINE/SET PORT IP CSLIP Privilege: P

NOTE: A "Set" can only be done on the port you are currently on. All other ports are define only.

Use this command to specify whether or not the port can initiate communications with a remote device using Compressed SLIP (CSLIP) packets. When a port initiates activity on the SLIP link, and the use of compressed SLIP is enabled, the port will immediately begin transmitting compressed packets on the serial link.

SLIP links can transmit and receive packets that have been compressed using the Van Jacobson compression algorithm (refer to RFC 1144). Compression allows SLIP links to operate with higher throughput under some circumstances. The SLIP implementation also supports the transmission of uncompressed packets, since not all remote devices permit the use of compression. Use the DEFINE/SET PORT IP SLIP ENABLED command.

When the remote device initiates activity on the SLIP link, the port will automatically detect whether or not the remote device is using compressed SLIP packets. The port will use the same type (compressed or uncompressed) of packets as the remote device. The port will do this whether you have SLIP or CSLIP enabled.

A SLIP link can have a number of sessions (or slots), using higher-level protocols such as TCP/IP, operating across the link. This can happen, for example, when the SLIP link is used in a gateway configuration that supports several users, or in a configuration where a single node (such as a dial-in PC) is connected to the port and the single node has several windows in use. RFC 1144 allows a SLIP link to use a maximum of 16 slots. (This is because the compression mechanism is very memory intensive. If too many slots use compression, the access server or the remote device could run out of memory resources to perform other tasks.) When Van Jacobson compression is in use on a SLIP link, a Xyplex access server will allocate sufficient memory to support 16 slots (the maximum permitted), regardless of the number of slots that will actually be used on the link. If the remote device only supports fewer slots, that number will be the actual number of slots used on the link.

See the Using the TCP/IP Features section in the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE/SET PORT port-list IP CSLIP  [ENABLED]
                                    [DISABLED]
```

Where	Means
port-list	One or more access server ports where you want to enable/disable the IP CSLIP feature.
ENABLED	The port can initiate communications with a remote device using Compressed SLIP (CSLIP) packets.

DISABLED The port cannot initiate communications with a remote device using Compressed SLIP (CSLIP) packets. This is the default.

Example

```
DEFINE PORT IP CSLIP ENABLED
```

DEFINE/SET PORT IP SECURITY Privilege: P

The Internet Security feature lets you build a table of networks, subnets, and nodes that are either allowed or denied a Telnet connection to specified ports. In addition, specific ports can be restricted from connecting to an Internet address.

See the Security section of the *Advanced Configuration Guide* for a description of the Internet Security feature.

Note: *When you specify ALL ports for a security table entry, the entry does not apply to port 0 (the console port). To define/set security for Port 0, include the port in a port list (e.g., 0 - 16) or individually specify entries for Port 0.*

Syntax

```
DEFINE/SET PORT [port-list] IP SECURITY DEFAULT [INBOUND]   [ALLOW]
                                                            [DENY]
                                                [OUTBOUND]  [ALLOW]
                                                            [DENY]

DEFINE/SET PORT [port-list] IP SECURITY   [security-info]
```

where the following is the syntax for *security-information*:

```
[INBOUND [ALLOW] internet-addr MASK [SECURITY-MASK] [ENABLED]
         [DENY]                                     [DISABLED]

 [OUTBOUND] [ALLOW] internet-addr MASK [SECURITY-MASK]][ENABLED]
            [DENY]                                     [DISABLED]
```

Where	Means
INBOUND	The security table entry pertains to inbound connections (i.e., a connection initiated from the serial device connected to the port going to another device on the LAN).
OUTBOUND	The security table entry pertains to outbound connections (i.e., a connection initiated by another device on the network going to a serial device attached to the port.
ALLOW	The server should allow connections from or to the specified internet address.
DENY	The server should not allow connections from or to the specified internet address.

DEFINE/SET PORT IP SECURITY (continued)

DEFAULT	Specifies whether the server default for inbound or outbound connections is to allow or deny connections from or to the specified Internet address.
internet-addr	An internet address to which connections are allowed or denied.
MASK	Indicates that a network security mask follows.
secur-mask	Specifies how much of the internet address to use. If you do not specify a security mask for an Inbound entry, a network-specific mask will be used. If you specify neither ENABLED nor DISABLED for this setting, and a matching security entry exists, the *port-list* in the command will overwrite the *port-list* in the existing entry.
ENABLED	Add the port(s) to the existing *port-list* if a matching entry already exists in the Internet Security table.
DISABLED	Remove the port(s) from the *port-list* if a matching entry exists.

Examples

```
DEFINE PORT 1 IP SECURITY DEFAULT OUTBOUND DENY
```

```
DEFINE PORT 1 IP SECURITY OUTBOUND ALLOW 192.12.119.1 MASK 255.255.255.0 ENABLED
```

DEFINE/SET PORT IP SLIP Privilege: P

NOTE: A "Set" can only be done on the port you are currently on. All other ports are define only.

Use this command to enable or disable Serial Line Internet Protocol (SLIP) for specific ports.

You can only SET the IP SLIP to ENABLED for your own port. Use the DEFINE command to enable or disable SLIP for other ports.

See the Using the TCP/IP Features section in the *Advanced Configuration Guide* for a description of the SLIP feature.

This command does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT [port-list] IP SLIP [ENABLED]
                                    [DISABLED]
DEFINE/SET PORT [port-list] IP SLIP [slip-information]
```

where the following is the syntax for *slip-information*:

```
 [ADDRESS local-addr] REMOTE [remote-addr] MASK [slip-mask]
```

DEFINE/SET PORT IP SLIP (continued)

Where	Means
ENABLED	Enables SLIP for the specified port or *port-list*.
DISABLED	Disables SLIP for the specified port. To use this keyword, you must use a DEFINE command. This is the default setting.
ADDRESS	Assign a specific internet-address to port. If you enable SLIP without setting the port's internet address, the server will obtain the internet address when it receives its first packet from the remote server. No users on the network will be able to initiate a connection with the remote server until the server receives at least one packet from the remote server.
local-addr	The Internet address you are assigning to the server port.
REMOTE	Specifies that a remote Internet address follows.
remote-addr	The remote Internet address to which the *local-address* corresponds. (When this address is on a different network, you define this correlation in the server's static routing table; e.g., using the DEFINE SERVER IP ROUTE command.)
MASK	Specifies that a network mask, corresponding to the *remote-address*, follows.
slip-mask	Specifies how much of the remote IP address to use. In most cases, this should be set to 255.255.255.255 to prevent ARPing on the port.

Examples

```
DEFINE PORT 1-5 IP SLIP ENABLED

DEFINE PORT 1 IP SLIP ADDRESS 192.12.119.72 REMOTE 192.12.130.1 MASK
255.255.255.255
```

DEFINE/SET PORT IP SLIP AUTOSEND Privilege: P

Use this command to enable/disable automatic sending of SLIP address information. With this command enabled, the following addresses are returned when you issue the `SET PORT IP SLIP ENABLE` command:

- SLIP remote address
- SLIP local address
- SLIP Mask address

Use the SHOW PORT ALT CHARACTERISTICS command to display the current status of SLIP Autosend.

***Note**: A "Set" can only be done on the port you are currently on. All other ports are define only.*

Syntax

```
DEFINE PORT <port-list> IP SLIP AUTOSEND [ENABLED]
                                         [DISABLED]
```

Where	Means
ENABLED	Allow SLIP addresses to be automatically sent.
DISABLED	Do not allow SLIP addresses to be automatically sent.

Example

```
DEFINE PORT 4 IP SLIP AUTOSEND ENABLED
```

DEFINE/SET PORT IP TCP KEEPALIVE TIMER Privilege: P

You can specify a TCP keepalive timer, which functions like the LAT keepalive timer. When this feature is enabled, the access server periodically transmits a null message to the partner of a session. If the Telnet partner does not respond during the length of time you specify, the access server disconnects the session.

You assign the keepalive timer to one or more ports. The value you set also specifies how often the server will attempt to reconnect a session when there is a connection failure, for ports that are also enabled for AUTOCONNECT. Use the SHOW/LIST PORTS ALTERNATE CHARACTERISTICS command to display the current setting of the TCP keepalive timer.

As you increase the size of the *timer-value*, you will lengthen the time for the server to determine when the connection partner has gone down. However, as you decrease the size of this value, you increase the amount of network traffic.

You cannot modify the keepalive timer while there is an active session on the port.

Syntax

```
DEFINE/SET PORT [port-list] IP TCP KEEPALIVE TIMER [timer-value]
```

Where	Means
IP	Define or change the length of time that the server will transmit a null message to the Telnet partner, when there is no other traffic originating at the server to the partner. The null message notifies circuit partner(s) that the server is still active.
timer-value	The number of minutes that the access server will wait for a response from the Telnet partner after transmitting the null message before terminating the session. Valid values are 0 through 30 minutes. The default is 0, which specifies that the keepalive timer is disabled.

Example

```
DEFINE PORT 5 IP TCP KEEPALIVE TIMER 20
```

DEFINE PORT IP TCP OUTBOUND ADDRESS Privilege: P

Use this command to configure a unique source IP address on a per-port basis for an outbound telnet connection (i.e., a connection initiated by the attached serial device going to another node on the network).

Note: *You cannot use this command for Port 0.*

Use the SHOW PORT ALT CHARACTERISTICS command to display the current OUTBOUND ADDRESS settings.

Syntax

```
DEFINE/SET PORT [port number] IP TCP OUTBOUND ADDRESS [ip-address]
```

Where	Means
ip-address	The unique source IP address for the port's outbound connection. The default is 0.0.0.0. If you use the default setting, the server's IP address is used as the source IP address, otherwise the source address is the TCP outbound address.

Example

```
DEFINE PORT 5 IP TCP OUTBOUND ADDRESS 179.144.122.3
```

DEFINE/SET PORT IP TCP WINDOW SIZE Privilege: P

Use this command to specify the size of the TCP window to be used by a TCP/IP session. A typical TCP/IP session requires about [1600 + (3 * *TCP_window_size*)] bytes. The window size used for a session is that which is in effect when the session starts.

If you connect a printer to a serial port, and the printer's performance appears to be slow, you might need to increase the TCP window size for that port.

Note: *Increasing this value will decrease the amount of free memory on your server. Verify that the server has sufficient memory remaining in order to operate properly.*

Syntax

```
DEFINE/SET PORT [port-list]  IP TCP WINDOW SIZE [tcp-window-size]
```

Where	Means
tcp-window-size	The size of TCP window. Valid values for size are between 64 and 8192 bytes. The default value is 256.

Example

```
DEFINE PORT 5 IP TCP WINDOW SIZE 512
```

DEFINE/SET PORT INTERRUPTS Privilege: P

Use this command to specify whether a local user can interrupt a remote session at a port, by entering the local switch (or BREAK) character. When the remote session is interrupted, the port will enter the local command mode. (The remote session can be resumed using the local command mode RESUME command.)

An example of this occurs when a port is connected to a hard-copy terminal, which has been set up to accept print jobs that are initiated from elsewhere on the network. This determines whether or not a user can interrupt a session, in this case another user's print job, by typing the local switch character or pressing the BREAK key at the hard-copy terminal.

This command only applies if the PORT ACCESS is set to DYNAMIC.

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT [port-list] INTERRUPTS    [DISABLED]
                                          [ENABLED]
```

Where	Means
DISABLED	Local users cannot interrupt a remote session at the port by entering the local switch character. This is the default setting.
ENABLED	Local users can interrupt a remote session at a port by entering the local switch character.

Example

```
DEFINE PORT 5 INTERRUPTS ENABLED
```

DEFINE/SET PORT IP FILTER Privilege: P

IP traffic filters determine which IP sources and destinations can communicate with each other through the access server's ports. You can define these filters on the LAN interface or on individual ports. Configure filters on a per-port basis when users/clients gain access to the server through a network protocol, such as SLIP or PPP.

The access server applies the filters to IP packets as it *receives* them from the attached LAN or specified port(s).

A traffic filter specifically allows or restricts traffic between two points; for example, between a dial-in client and a network host. Traffic filters also determine which IP protocols the access server can forward, or they can allow or restrict communication through specific TCP and UDP ports.

Additionally, IP filters can allow or restrict forwarding of TCP packets when the packet's SYN bit is set to ON and the ACK bit is set to OFF. This bit pattern indicates that the sender is trying to establish a new session with a destination port. By discarding packets with this bit pattern, you prevent remote users from establishing sessions with hosts on the local network.

Note: *When IP traffic filtering is enabled, only TCP packets that have a complete TCP header are passed. This eliminates potential security breaches that can occur when packets are fragmented and the initial fragment does not include the SYN flag.*

Enabling IP Filtering

By default, IP traffic filtering is disabled. You can specify any of the following criteria to filter IP traffic:

- IP protocol type: a specific protocol ID, TCP, UDP, or ALL
- Destination IP address and subnet mask
- Destination port number or range of numbers
- Source port number or range of numbers
- Source IP address and subnet mask
- Whether a TCP packet has its SYN bit ON and its ACK bit OFF

See the section in the *Advanced Configuration Guide* that discusses IP Filtering for more information.

DEFINE/SET PORT IP FILTER (continued)

Syntax

DEFINE/SET PORT [*port-list*] IP FILTER [*criteria-information*] [*filter-instructions*]

Example

DEFINE PORT 2,3,5 IP FILTER DESTINATION PORT 23 DESTINATION 192.168.23.122 DISCARD

DEFINE/SET PORT IP FILTER PROTOCOL Privilege: P

When an inbound IP packet is neither TCP nor UDP, the server ignores any filters that specify an individual TCP or UDP port, or range of ports. If it receives a packet that has multiple matching filters, the server applies the most specific filter.

See the section that discusses IP Settings in the *Basic Configuration Guide* for more information.

Use the following command to specify the IP filtering protocols:

```
DEFINE/SET PORT port-list IP FILTER PROTOCOL   [protocol-id]       [DISCARD]
                                               [TCP]              [FORWARD]
                                               [UDP]
                                               [ALL]
```

Where	Means
protocol-id	Specify a port number from 0 to 255.
TCP	Sets the port to accept only TCP packets.
UDP	Sets the port to accept only UDP packets.
ALL	Sets the port to accept all protocol types (UDP and TCP). This is the default.
DISCARD	The port will discard protocol types that do not match the criteria
FORWARD	The port will accept all protocol types that match the criteria.

EXAMPLE

```
DEFINE PORT 5 IP FILTER PROTOCOL TCP DISCARD
```

DEFINE/SET PORT IP FILTER DESTINATION PORT Privilege: P

If you use this filtering option, the server looks for matching filters that specify the destination IP subnet (i.e., the filter destination mask ANDed with the filter destination address matches the packet destination address ANDed with the filter destination mask). If only one filter specifies the largest destination IP subnet mask, the server applies that filter.

If more than one of the remaining filters specify the largest destination IP subnet mask, the server looks for matching filters that specify the source IP subnet (i.e., the filter source mask ANDed with the filter source address matches the packet source address ANDed with the filter source mask). At this point only one filter should remain; the server applies that filter.

See the Using TCP/IP Features section in the *Advanced Configuration Guide* for more information.

Use the following command to specify the destination IP address and subnet mask or destination port number or range of numbers.

```
DEFINE/SET PORT port-list IP FILTER DESTINATION PORT [port number]
                                                     [port number - port number]

                                                     [ALL]
```

Where	Means
port number	The destination port's number. Valid values are from 0 to 65535.
port number - port number	Specify a range of destination port numbers.
ALL	Specify all port numbers. This is the default setting.

Example

```
DEFINE PORT IP FILTER DESTINATION PORT 3-7
```

If more than one of the remaining filters specify the narrowest destination TCP/UDP port range, the access server looks for filters that specify a TCP SYN value (ON or OFF). If only one filter specifies a TCP SYN value, the server applies that filter.

If more than one of the remaining filters specify a TCP SYN value, the access server looks for filters that specify the range of source TCP or UDP ports. When multiple filters specify an equal range of port numbers, the server looks for filters with the lowest beginning port number.

If only one matching filter specifies the narrowest range of source TCP/UDP ports, the server applies that filter.

See the section that discusses IP Settings in the *Advanced Configuration Guide* for more information.

Use the following command to specify whether a TCP packet has its SYN bit ON and its ACK bit OFF.

```
DEFINE/SET PORT port-list IP FILTER SYN   [ON]  [DISCARD]
                                          [ALL] [FORWARD]
```

Where	Means
ON	The SYN (synchronization) bit is set to ON and the ACK (acknowledge) bit is set to OFF in the TCP header.
ALL	Any value for the SYN and ACK bits. This is the default setting.
DISCARD	The port will discard all packets that do not match the criteria
FORWARD	The port will accept all packets that match the criteria.

Example

```
DEFINE PORT 5 IP FILTER SYN ON DISCARD
```

DEFINE/SET PORT IP FILTER SOURCE PORT Privilege: P

Use the following command to specify the source port number or range of port numbers or the IP address and subnet mask.

Syntax

```
define/set Port port-list ip filter SOURCE PORT [port number] [DISCARD]
                                                [port number-port number][FORWARD]
                                                [ALL]                    [DISCARD]

DEFINE/SET PORT port-list IP FILTER SOURCE[ip-address [MASK subnet-mask]]
                                          [ALL]
```

Where	Means
Source Port	The source port number.
port number	A port number from 0 to 65535.
port number - port number	The range of port numbers
ALL	Any port. This is the default setting.
DISCARD	The port will discard all packets that do not match the criteria
FORWARD	The port will accept all packets that match the criteria.
ip-address	The source IP address
MASK *subnet-mask*	The source port's MASK and subnet mask. If the keyword MASK is omitted, the default mask characteristic (Natural Class mask) is used.

Example

```
DEFINE PORT 2,4,7 IP FILTER SOURCE PORT 5-6 DISCARD
```

DEFINE/SET PORT IP FILTER DESTINATION Privilege: P

Use the following command to specify the destination IP address and subnet mask.

Syntax

```
DEFINE/SET PORT port-list IP FILTER DESTINATION   [ip-address[MASK subnet-mask]]
                                                  [ALL]          [DISCARD]
                                                                 [FORWARD]
```

When	Means
DESTINATION	Defines the traffic filter.
ip-address	The destination port's IP address.
MASK *subnet-mask*	The destination port's MASK and subnet mask. If the keyword MASK is omitted, the default mask characteristic (Natural Class mask) is used.
ALL	Any destination.
DISCARD	The port will discard all packets that do not match the criteria
FORWARD	The port will accept all packets that match the criteria.

Example

```
DEFINE/SET PORT 3 IP FILTER DESTINATION 179.132.122.4 MASK 255.255.255.255 ALL
```

By default, IPX traffic filtering is disabled. Use the DEFINE SERVER IPX FILTERING command to enable this feature before you define the specific traffic filters for access server ports. You configure traffic filters on a server and/or individual port basis. The server applies them to packets as it receives them.

IPX traffic filters determine which IPX sources and destinations can communicate with each other through the access server's ports. A traffic filter specifically allows or restricts traffic between two points, for example between two networks or between a NetWare client and server.

The IPX protocol specification requires that IPX networks be identified by a network number. This permits efficient routing of packets to their destinations. Each device in a given IPX network must know its network number. Access servers can obtain a network number in one of two ways: the server can "learn" its network number from other IPX devices (such as a Novell file server) that is connected to the same Ethernet network, or the server administrator can assign a network number.

An access server uses a minimum of three unique network numbers. One network number is used for traffic that is sent or received on the Ethernet network. Another network number is used for traffic that is sent over a given PPP link (setting this up is covered later), and a third network number is an "internal" network number, which is used inside the server for transferring information between the Ethernet network and the PPP link(s). The internal network number must not be used elsewhere in the Novell NetWare network (i.e., must be unique).

You can specify the following criteria in a traffic filter:

- Destination IPX network and/or Ethernet address
- Source IPX network and/or Ethernet address

Syntax

Use these commands to define IPX traffic filters:

```
DEFINE PORT port-list IPX FILTER destination-criteria       [FORWARD]
                                                            [DISCARD]

DEFINE PORT port-list IPX FILTER source-criteria            [FORWARD]
                                                            [DISCARD]

DEFINE PORT port-list IPX FILTER destination-criteria source-criteria
                                                            [FORWARD]
                                                            [DISCARD]
```

The *destination-criteria* can include:

```
DESTINATION NETWORK [ipx-network]
                    [ALL]

DESTINATION NODE    [node-address] (e.g., 08008712AB34)
                    [ALL]
```

The *source-criteria* can include:

```
SOURCE NETWORK [ipx-network]     [DISCARD]
               [ALL]             [FORWARD]

SOURCE NODE  [node-address] (e.g., 08008712ABCD)     [DISCARD]
             [ALL]                                   [FORWARD]
```

Note: *Use the SHOW SERVER IPX RIP STATUS and SHOW SERVER IPX SAP STATUS commands to display the current IPX node addresses.*

Where	Means
network-number	The IPX network number for the port (i.e., the PPP link). Valid values for network-number are hexadecimal numbers between 0 (the default) and FFFFFFFE. A network-number of 0 means that the port will learn its network number from the remote PPP device(s), or the server administrator can assign a network number. The network number cannot be used elsewhere in the network.
ipx-network	A specific IPX socket or network destination.
node-address	The IPX network number for the port (i.e., the PPP link). Valid values for network-number are hexadecimal numbers between 0 (the default) and FFFFFFFE.

destination-criteria	Enter one of the following commands:
	`DESTINATION NETWORK [ipx-network]`
	`[ALL]`
	
	`DESTINATION NODE [node-address]`

DEFINE/SET PORT [PPP] IPX (continued)

source-criteria Enter one of the following commands:

```
SOURCE NETWORK [ipx-network]
               [ALL]

SOURCE NODE [node-address]
            [ALL]
```

ALL All traffic from the specified source.

FORWARD The traffic from the specified ports will be forwarded to the file server(s). This is the default.

DISCARD If this command is used with ALL. All traffic will be discarded that is not from a specified source.

Examples

```
DEFINE PORT IPX NETWORK FFFFFFFD

DEFINE PORT ALL IPX FILTER DESTINATION NETWORK ALL DISCARD

DEFINE PORT 5 IPX FILTER DESTINATION NODE ALL DISCARD

DEFINE PORT 5 IPX FILTER DESTINATION NODE ALL SOURCE NODE ALL DISCARD

DEFINE PORT ALL IPX FILTER SOURCE NETWORK ALL DISCARD

DEFINE PORT 5 IPX FILTER SOURCE NODE ALL DISCARD
```

DEFINE PORT IPX RIP IMPORT — Privilege: P

When the IPX protocol is enabled, the access server adds all routes that it learns through RIP to its IPX route table by default. This process is called *importing*. The server also advertises all routes in its IPX route table to other IPX routers, by default. This process is called *exporting*.

Syntax

```
DEFINE PORT [port-list] IPX RIP IMPORT NETWORK [network]     [ACCEPT]
                                               [ALL]         [DISCARD]
```

Where	Means
network	A hexadecimal value from 1 to fffffffe.
ALL	All networks.
ACCEPT	Accept all routes
DISCARD	Prevent traffic from specified routes.

Example

```
DEFINE PORT 5 IPX RIP IMPORT NETWORK ALL ACCEPT
```

DEFINE/SET PORT IPX RIP BROADCAST Privilege: P

This command specifies whether or not the server will broadcast RIP information over the serial link to the remote partner, and if the information is broadcast, how much information the server will send.

In some network configurations, an access server operates as an asynchronous IPX router. IPX routers exchange information about the networks to which they are attached, and the networks they can reach, through Router Information Protocol (RIP) packets. IPX routers use RIP information to route IPX packets. Each IPX router maintains a table of RIP information that it has received from other routers. IPX routers also broadcast RIP packets to neighboring routers periodically.

Several commands are available which control the broadcasting and storage of RIP information.

Syntax

```
DEFINE/SET PORT port-list IPX RIP [BROADCAST]   [FULL]
                                                [CHANGE]
                                                [NONE]
```

Where	Means
FULL	The server will broadcast the entire contents of the RIP table.
CHANGE	The server will only broadcast new or changed routing information. The is the default.
NONE	The server will not broadcast any routing information.

Example

```
DEFINE PORT 5 IPX RIP BROADCAST FULL
```

DEFINE/SET PORT IPX RIP [BROADCAST] DISCARD TIMEOUT Privilege: P

This command specifies how long the server keeps RIP information that it receives over the serial link to the remote partner.

There are several commands available that control the broadcasting and storage of RIP information.

Syntax

DEFINE/SET PORT *port-list* IPX RIP [BROADCAST] DISCARD TIMEOUT *timer-multiple*

Where	Means
timer-multiple	Specfies how long the server keeps RIP information that it receives over the serial link to the remote partner. The *timer-multiple* that you specify is multiplied by the value specified for the DEFINE/SET SERVER IPX RIP BROADCAST TIMER *time* command. Valid values for *timer-multiple* are whole numbers between 0 and 4294967295. The default is 3.

Example

```
DEFINE PORT 5 IPX RIP BROADCAST DISCARD TIMEOUT 5
```

DEFINE/SET PORT IPX RIP BROADCAST TIMER Privilege: P

This command specifies how frequently the access server will broadcast RIP information over the serial link to the remote partner.

Several commands are available which control the broadcasting and storage of RIP information.

Syntax

DEFINE/SET PORT *port-list* IPX RIP [BROADCAST] TIMER <*timer*>

Where	Means
timer	The frequency at which the access server will broadcast RIP information over the serial link to the remote partner. Valid values are whole numbers between 0 and 4294967295 (seconds). The default interval is 60 seconds.

Example

```
DEFINE PORT 5 IPX RIP BROADCAST TIMER 60
```

DEFINE/SET PORT IPX RIP EXPORT NETWORK Privilege: P

When the IPX protocol is enabled, the access server adds all routes that it learns through RIP to its IPX route table by default. This process is called *importing*. The server also advertises all routes in its IPX route table to other IPX routers, by default. This process is called *exporting*.

See the DEFINE SERVER IPX RIP EXPORT command to specify the server settings.

Syntax

```
DEFINE/SET PORT [port-list] IPX RIP EXPORT NETWORK   [network]    [ADVERTISE]
                                                     [ALL]        [HIDE]
```

Where	Means
network	A hexadecimal value from 1 to ffffffe.
ALL	Export all networks
ADVERTISE	The server will display all routes in its IPX route table to other IPX routers. Default.
HIDE	The server's IPX route table will not be displayed to other IPX routers.

Example

```
DEFINE PORT 5 IPX RIP EXPORT NETWORK ALL ADVERTISE
```

DEFINE/SET PORT IPX SAP EXPORT NETWORK Privilege: P

When the IPX protocol is enabled, the access server advertises all service names and types in its SAP table to other IPX routers, by default. This process is called *exporting*.

Syntax

```
DEFINE/SET PORT [port-list] IPX SAP EXPORT NETWORK [network]   [ADVERTISE]
                                                   [ALL]       [HIDE]
```

Where	Means
network	A hexadecimal value from 1 to fffffffe.
ALL	All service names and service types on the server's SAP table will display to other IPX routers.
ADVERTISE	All service names and service types on the server's SAP table will display to other IPX routers.
HIDE	Service names and service types on the server's SAP table will not display to other IPX routers.

Examples

```
DEFINE PORT ALL IPX SAP EXPORT NETWORK ALL HIDE

DEFINE PORT 5 IPX SAP EXPORT NETWORK ALL ADVERTISE
```

DEFINE/SET PORT IPX SAP EXPORT TYPE Privilege: P

Use this command to identify the NetWare service types such as a file server, printer, etc. in the SAP table.

Syntax

```
DEFINE/SET PORT [port-list] IPX SAP EXPORT TYPE [type-value]   [ADVERTISE]
                                                [ALL]          [HIDE]
```

Where	Means

type-value

type-value	**Description**
0	Unknown
1	User
2	User Group
3	Print Queue
4 or 278	File Server
5	Job Server
6	Gateway
7	Print Server
8	Archive Queue
9	Archive Server
A	Job Queue
B	Administration
24	Remote Bridge Server
47	Advertising Printer Server
107	Server (internal)

ALL	All service types will be displayed to other routers.
ADVERTISE	All service types will be displayed to other routers.
HIDE	All service types will not be displayed to other routers.

Examples

```
DEFINE PORT 5 IPX SAP EXPORT TYPE ALL ADVERTISE

DEFINE PORT ALL IPX SAP EXPORT NETWORK 1234 TYPE 6 ADVERTISE
```

DEFINE/SET PORT IPX SAP IMPORT NETWORK Privilege: P

Use this command to identify the source or destination network.

Syntax

```
DEFINE/SET PORT [PORT-LIST] IPX SAP IMPORT NETWORK [NETWORK] [ACCEPT]
                                                   [ALL]     [DISCARD]
```

Where	Means
network	The source or destination network. It is a hexadecimal value from 1 to fffffffe.
ALL	All networks.
ACCEPT	Accept all routes
DISCARD	Prevent traffic from specified routes.

Example

```
DEFINE PORT 5 IPX SAP IMPORT NETWORK ALL ACCEPT
```

DEFINE/SET PORT IPX SAP IMPORT TYPE Privilege: P

Use this command to identify the type of service to import such as file servers, printers, etc.

Syntax

```
DEFINE/SET PORT [port-list] IPX SAP IMPORT TYPE [type-value] [ACCEPT]
                                                [ALL]        [DISCARD]
```

Where	Means

type-value

type-value	**Description**
0	Unknown
1	User
2	User Group
3	Print Queue
4 or 278	File Server
5	Job Server
6	Gateway
7	Print Server
8	Archive Queue
9	Archive Server
A	Job Queue
B	Administration
24	Remote Bridge Server
47	Advertising Printer Server
107	Server (internal)

ALL	All networks.
ACCEPT	Accept all routes
DISCARD	Prevent traffic from specified routes.

Example

```
DEFINE PORT 5 IPX SAP IMPORT TYPE ALL ACCEPT
```

DEFINE PORT KERBEROS Privilege: P

Use this command to specify whether the port is to provide Kerberos user verification as part of the login process.

***Note**: There is no SET command for this feature.*

Port 0 is not included when you specify ALL ports. To enable Kerberos user verification for the console port (Port 0), you must specifically list Port 0 when you issue the DEFINE PORT KERBEROS command.

See the Security Features section in the *Advanced Configuration Guide* for a description of Kerberos support.

***Note:** See the DEFINE/SET PORT OUTBOUNDSECURITY command for remote and dynamic ports.*

Syntax

```
DEFINE/SET PORT port-list KERBEROS  [ENABLED]
                                    [DISABLED]
```

Where	Means
ENABLED	The port is to provide Kerberos user verification.
DISABLED	The port will not provide Kerberos user verification. This is the default.

Example

```
DEFINE PORT 5 KERBEROS ENABLED
```

DEFINE/SET PORT KEYMAP Privilege: S, N, P

Use this command to assign an individual copy of a TN3270 keymap to this port and change the escape sequences in the keymap. The access server uses the keymap information from the device specified by the TN3270 DEVICE setting for this port. The KEYMAP setting is only valid with the SET command *and* the SERVER TN3270 PORT KEYMAPS command set to ENABLED.

See the Using the TN3270 Features section in the *Advanced Configuration Guide* for information about TN3270 support.

Syntax

```
DEFINE/SET PORT port-list KEYMAP [key "escape-seq" "description"]
                                 [NONE]
```

Where	Means
key	An IBM 3270 display station function. See the *Configuration Guide* for a list of IBM display station functions to use in this variable.
"*escape-seq*"	The byte sequence from the local terminal that the access server maps to the IBM display station function in the key variable. You can specify the characters in the byte sequence in two ways: enter the hexadecimal values, which you obtain from the Programmer's Reference manual for the local terminal, or manually press the keys on the terminal. You can use from 0 to 9 hexadecimal values in this variable, and enclose the variable in quotes.
"*description*"	A text description.Describes the keymap escape sequence in different keymap displays. These include SHOW PORT KEYMAP and the display that appears when the user presses the SHOWKEYS status key during TN3270 terminal emulation. You can use from 0 to 9 characters in this variable, and enclose the variable in quotes.
NONE	Specifies that this port does not have an individual keymap assigned to it. Use this keyword to remove a previously assigned keymap.

Example

```
DEFINE PORT 5 KEYMAP PF1 "01 40 13" "F1"
```

DEFINE PORT LAT DEDICATED SERVICE Privilege: P

Use this command to assign a LAT service to which the port is permanently assigned, or to change or remove the current permanent service assignment for the port. This setting automatically connects the port to the dedicated service, whenever a user logs on to that port.

Note: *You can only use a DEFINE command to specify the PORT LAT DEDICATED SERVICE setting. See the DEFINE PORT DEDICATED SERVICE command for more information.*

Syntax

```
DEFINE/SET PORT port-list LAT DEDICATED service [service-name]     [NODE]
                                                 [node name][DESTINATION][port name]
                                                 [NONE]

                                                 [NONE]     [DESTINATION] [port name]
                                                 [NONE]

                                                 [NONE][NODE][node name]
                                                 [DESTINATION][port name]
                                                 [NONE]

                                                 [NONE][DESTINATION] [port name]
                                                 [NONE]
```

Where	Means
service-name	The name of the LAT service to which the port is permanently assigned.
NODE	Specifies that you will set or change the name of the node on which the dedicated service is offered.
node name	The name of the LAT service node at which the dedicated service is offered.
DESTINATION	Specifies that you will set or change the name of the server port at which the dedicated service is offered.
port name	The name of the server port at which the service, specified by the *service-name*, is offered.
NONE	Specifies that this port, all ports, or the ports listed in the *port-list* will not have a dedicated service, or that you wish to cancel a previously-defined dedicated service, service node, or destination server port. This is the default setting.

Example

```
DEFINE PORT 5 LAT DEDICATED SERVICE VMSHOST
```

DEFINE/SET PORT LAT PREFERRED SERVICE Privilege: N, P

Use this command to assign a LAT service to which the port will connect whenever a user makes a connect request without specifying a service, or to change or remove the current preferred service assignment for the port.

Syntax

```
DEFINE/SET PORT [port-list]  LAT PREFERRED SERVICE [service-information]
```

The *service-information* can include the following criteria.

```
[service-name] [NODE][node name][DESTINATION]  [port name] [CONTROLLED]
[NONE]
[NONE] [DESTINATION][port name]
[NONE]
[NONE] [NODE] [node name]  [DESTINATION][port name]
[NONE]
[NONE] [DESTINATION][port name]
[NONE]
```

Where	Means
service-name	The name of the LAT service to which the port whenever a user makes a connect request without specifying a service.
NODE	The name of the node on which the preferred service is offered.
node name	The name of the service node at which the preferred service is offered.
DESTINATION	The name of the server port at which the preferred service is offered.
port name	The name of the server port at which the service, specified by the service-name, is offered.
NONE	The ports listed in the port-list will not have a preferred service, or that you wish to cancel a previously defined preferred service, service node, or destination server port. This is the default setting.
CONTROLLED	Frames a session with string specified by the DEFINE/SET PORT CONTROLLED SESSION INITIALIZE|TERMINATE command.

Example

```
DEFINE PORT 5 LAT PREFERRED SERVICE FINANCEVAX
```

DEFINE/SET PORT LIMITED VIEW — Privilege: P

Use this command to enable or disable node and service display restrictions for secure and non-privileged users. Specifically, these users cannot view the SHOW/LIST NODES or SERVICES displays.

This feature does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT [port-list] LIMITED VIEW  [ENABLED]
                                          [DISABLED]
```

Where	Means
VIEW	An optional keyword.
ENABLED	Specifies that a secure or non-privileged user(s) at the port(s) listed in the *port-list* cannot view SHOW/LIST NODES or SERVICES displays.
DISABLED	Specifies that a secure or non-privileged user(s) at the port(s) listed in the *port-list* can view SHOW/LIST NODES or SERVICES displays. This is the default.

Example

```
DEFINE PORT 5 LIMITED VIEW ENABLED
```

DEFINE/SET PORT LINE EDITOR Privilege: N, P

Use this command to define, change, or delete a line editing character, or enable or disable the command line editing feature. Use the SHOW/LIST MONITOR LINE EDITOR CHARACTERISITCS command to display the current settings.

Note: This command does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list  LINE EDITOR     [ENABLED]
                                           [DISABLED]

                                           [BACKSPACE]        [character]
                                                              [NONE]
                                           [BEGINNING]        [character]
                                                              [NONE]
                                           [CANCEL]           [character]
                                                              [NONE]
                                           [DELETE BEGINNING] [character]
                                                              [NONE]
                                           [DELETE LINE]      [character]
                                                              [NONE]
                                           [END]              [character]
                                                              [NONE]
                                           [FORWARDS]         [character]
                                                              [NONE]
                                           [INSERT TOGGLE]    [character]
                                                              [NONE]
                                           [NEXT LINE]        [character]
                                                              [NONE]
                                           [PREVIOUS LINE]    [character]
                                                              [NONE]
                                           [QUOTING CHARACTER] [character]
                                                              [NONE]
                                           [REDISPLAY]        [character]
                                                              [NONE]
```

DEFINE/SET PORT LINE EDITOR (continued)

Where	Means
DISABLED	The command line editing feature will not be available at the specified port(s).
ENABLED	The command line editing feature will be available at the specified port(s)
BACKSPACE	Define, change, or delete the line editing character that will move the cursor one position to the left. The command character you define will be ignored by ports whose PORT TYPE is set to HARDCOPY.
BEGINNING	Define, change, or delete the line editing character that will place the cursor at the beginning of the current command line. The command character you define will be ignored by ports whose PORT TYPE is set to HARDCOPY.
CANCEL	Define, change, or delete the line editing character that will cancel an interactive operation (such as changing a password), or delete the current command line.
DELETE BEGINNING	Define, change, or delete the line editing character that will delete everything on the current command line, from the cursor position to the beginning of the line.
DELETE LINE	Define, change, or delete the line editing character that will delete the current command line.
END	Define, change, or delete the line editing character that will place the cursor at the end of the current command line. The command character you define will be ignored by ports whose PORT TYPE is set to HARDCOPY.
FORWARD	Define, change, or delete the line editing character that will move the cursor one position to the right. The command character you define will be ignored by ports whose PORT TYPE is set to HARDCOPY.
INSERT TOGGLE	Define, change, or delete the line editing character that alternates between the insert character and overstrike character modes of operation. The command character you define will be ignored by ports whose PORT TYPE is set to HARDCOPY.
NEXT LINE	Define, change, or delete the line editing character that will recall the next command in the command history.
PREVIOUS LINE	Define, change, or delete the line editing character that will recall the previous command in the command history.
QUOTING CHARACTER	Define, change, or delete the line editing character that will quote the next character.

DEFINE/SET PORT LINE EDITOR (continued)

REDISPLAY — Define, change, or delete the line editing character that will re-display the current command line. The command character you define will be ignored by ports whose PORT TYPE is set to HARDCOPY.

character — A keyboard character that the user will type to perform the specified line editing function. It is recommended that you specify an unused CTRL character. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, or with the character you set for the PORT BACKWARD SWITCH or FORWARD SWITCH characteristics, or any Telnet command characters, or line-editor characters). If you do specify a CTRL character, when you type the character, it will be displayed as ^<Key> (i.e., if you type CTRL/B, the terminal will echo the characters: ^B).

NONE — There will not be a character that the user can type to perform the specified line editing function. Use this command to remove a previously-defined line editing character.

Example

```
DEFINE PORT 5 LINE EDITOR REDISPLAY ^B
```

DEFINE/SET PORT LOCAL SWITCH Privilege: N, P

Use this command to specify whether or not there will be a character that allows a user to return to the local command mode.

This setting does not apply to parallel ports.

Note: *Using the local switch does not disconnect the session it causes the session to run in the background. To resume the session, see the RESUME, DISCONNECT or KILL commands.*

Syntax

```
DEFINE/SET PORT port-list LOCAL SWITCH [character]
                                       [NONE]
```

Where	Means
character	A keyboard character that the user will type to return to the local command mode. It is recommended that you specify an unused CTRL character. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, or with the character you set for the PORT BACKWARD SWITCH or FORWARD SWITCH characteristics, or any Telnet command characters, or line-editor characters). If you do specify a CTRL character, when you type the character, it will be displayed as ^<Key> (i.e., if you type CTRL/B, the terminal will echo the characters: ^B).
NONE	There will not be a character that the user can type to return to the local command mode. This command can be used to remove a previously-defined local switch character. This is the default setting.

Example

```
DEFINE PORT 5 LOCAL SWITCH ^B
```

DEFINE/SET PORT LOGIN DURATION Privilege: P

Use this command to limit the time a user can remain logged in to a port, regardless of the activity on the port.

Syntax

```
DEFINE/SET PORT [port-list] LOGIN DURATION [timer]
```

Where	Means
timer	A value from 0 to 480, where 0 is disabled and 1-480 is the number of minutes.

Example

```
DEFINE PORT 5 LOGIN DURATION 30
```

DEFINE/SET PORT LOSS NOTIFICATION Privilege: S, N, P

Use this command to specify whether or not the server sends a Bell character to the device connected to the port, whenever input data (from the device) are lost due to a receive data error or a receive overrun error. (For example, the server will have the terminal beep when the user types a command line that exceeds 132 characters in length.)

Syntax

```
DEFINE/SET PORT port-list LOSS NOTIFICATION  [DISABLED]
                                             [ENABLED]
```

Where	Means
DISABLED	The server will not send a Bell character to the device attached to the port, whenever input data are lost.
ENABLED	The server will send a Bell character to the device connected to the port, whenever input data are lost. This is the default.

Example

```
DEFINE PORT 5 LOSS NOTIFICATION DISABLED
```

DEFINE/SET PORT MENU — Privilege: P

Use this command to enable a simple menu interface at a port. Once you enable the menu for a port, a non-privileged user at that port can only perform operations by choosing menu items. (A privileged user can disable the port menu from a different port, where the menu is not enabled.)

See the Menu section in the *Basic Configuration Guide* for a description of the Simple Menu Interface feature.

Syntax

```
DEFINE/SET PORT port-list MENU   [ENABLED]
                                 [DISABLED]
```

Where	Means
ENABLED	Enables the menu for the specified port or port-list.
DISABLED	Disables the menu for the specified port or *port-list*. This is the default setting.

Example

```
DEFINE PORT 5 MENU ENABLED
```

DEFINE/SET PORT MESSAGE CODES — Privilege: N, P

Use this command to specify whether or not, when status or error messages are displayed, the associated message code or message number is shown, or only the text of the message is shown.

Syntax

```
DEFINE/SET PORT port-list MESSAGE CODES  [DISABLED]
                                        [ENABLED]
```

Where	Means
DISABLED	Message codes or numbers will not be shown when status or error messages are displayed (i.e., only the message is displayed).
ENABLED	Message codes or numbers will be shown when status or error messages are displayed. This is the default setting.

Example

```
DEFINE PORT 5 MESSAGE CODES DISABLED
```

DEFINE/SET PORT MODEM CONTROL Privilege: P

Use this command to specify whether or not modem control signals and related PORT settings (e.g., DSRWAIT and DTRWAIT) are enabled at the port(s) listed in the *port-list* or all ports. The following table lists the cabling types and modem/flow control supported for each.

Cabling Type	Modem Control	Hardware Flow Control	Products
6-wire	X	NO	MX-TSERV-J8, MX-TSRVM-J8, and MX2120 Access Server cards.
7-wire	X	NO	MAXserver 1100,1120,1500,1520, 1800, and 1820 Access Servers.
8-wire	X	X	MAXserver 800, 1600,1604, 1608, 1620, 1640 Access Servers. Network 9000 Access Server 720 RJ-45 I/O Modules (Model 723).

See the *Getting Started Guide* supplied with your unit for a description of associated cabling issues. See the Modems section of the *Basic Configuration Guide* for information about modem control and setting up modems.

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list MODEM CONTROL   [DISABLED]
                                          [ENABLED]
```

Where	Means
DISABLED	Modem control signals are not enabled at the port(s) listed in the *port-list* or all ports. This is the default setting. This is typically used in a "data-leads-only" mode. With devices that use data-leads-only mode, only data, and no status signals, are exchanged between the device and the port. Data-leads-only mode is typically used with equipment that support limited EIA interface signals.
ENABLED	Modem control signals are enabled at the port(s) listed in the *port-list* or all ports.

Example

```
DEFINE PORT 5 MODEM CONTROL ENABLED
```

DEFINE/SET PORT MULTISESSIONS Privilege: N, P

Use this command to specify whether or not the port(s) listed in the *port-list* will support DEC terminals, such as the VT330 and VT420 models, which provide a feature called Dual Session Management. This feature enables users to display and control multiple simultaneous communication sessions. The sessions can be multiplexed (i.e., combined) onto a single serial line to a host.

Syntax

```
DEFINE/SET PORT port-list MULTISESSIONS   [ENABLED]
                                          [DISABLED]
```

Where	Means
ENABLED	The port(s) listed in the *port-list* will support terminals that use Dual Session Management.
DISABLED	The port(s) listed in the *port-list* will not support terminals that use Dual Session Management. This is the default setting.

Example

```
DEFINE PORT 5 MULTISESSIONS ENABLED
```

DEFINE/SET PORT NAME Privilege: P

Whenever a port is logged on, the server assigns the port a name. The default name is in the form: PORT_*port number*, where *port number* is the number of the physical server port. For example, the default name for port 1 of a server is PORT_1. Use the DEFINE/SET PORT NAME command to assign a different name to the port.

Syntax

DEFINE/SET PORT *port-list* NAME *port name*

Where	Means
port name	The new name for the specified port. The port name can be between 1 and 16 ASCII characters in length. (Note that the server will convert any lower-case letters to upper case.) Do not enclose the port name in quotation mark characters ("). The *port name* must be unique within each server. The default value for this variable is in the form: PORT_*port number*, where *port number* is the number of the physical server port .

Example

```
DEFINE PORT 5 NAME PRINTER-PORT
```

DEFINE/SET PORT NESTED MENU Privilege: P

Use this command to enable or disable this feature on a port, or specifies that this feature is required on the port. A user cannot access the Xyplex command interface at a port where nested menus are required.

You must specify a top-level menu number at ports where you enable or require the nested menu feature. The access server uses this number to determine which menu to display first.

If nested menus are required at a port, and the access server cannot find a menu file on the script server when the user attempts to log on to the port, the user cannot log on. When a user presses the <Exit> key at a port with nested menus required, the access server logs out the port. See the Nested Menus section of the *Configuration Guide* for more information.

Syntax

```
DEFINE/SET PORT port-list NESTED MENU    [ENABLED]
                                         [DISABLED]
                                         [REQUIRED]
```

Where	Means
port-list	One or more ports where you want to specify the status of the Nested Menu feature.
ENABLED	Nested menus are enabled, but not required at the ports you specify. If the access server cannot find the menu file, it opens the Xyplex command interface at these ports.
DISABLED	Disable the nested menu feature at the ports you specify.
REQUIRED	This port must use the nested menu feature or the interface logs out the port.

Example

This command enables nested menus on ports 6-8.

```
SET PORT 6-8 NESTED MENU ENABLED
```

DEFINE/SET PORT NESTED MENU TOP LEVEL Privilege: P

The DEFINE/SET PORT NESTED MENU TOP LEVEL command specifies the number of the highest-level menu for the ports you specify. The access server displays the highest-level menu first.

You must specify a top level menu number to use the Nested Menu Feature. If you do not, the access server cannot determine which menu to display first. If you do not specify this value, the access server issues an error message and does not display a menu when the user logs on to a port with Nested Menusenabled.

You specify menu numbers in the menu script with the `%menu_start` *n* "*menu-title*" command. The variable *n* indicates the menu number. See the Nested Menus section of the *Configuration Guide* for more information about this and other nested menu commands.

Syntax

```
DEFINE/SET PORT port-list NESTED MENU TOP LEVEL menu-number
```

Where	Means
port-list	One or more ports where you want to specify a top-level menu number.
menu-number	The number of the top level menu. Valid values are 0 through 255. The default is 0, which means that no top level menu is specified.

Example

This command specifies menu 1 as the top level menu for ports 5-10.

```
SET PORT 5-10 NESTED MENU TOP LEVEL 1
```

DEFINE/SET PORT NOLOSS — Privilege: N, P

Use this command to specify whether or not the port will store data in its typeahead buffer while waiting for a session connection to be made and then pass the data to the connection partner after the session connection is made.

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list NOLOSS    [DISABLED]
                                    [ENABLED]
```

Where	Means
DISABLED	The port will not store data in its typeahead buffer while waiting for a session connection to be made. When the NOLOSS is DISABLED, and the device connected to the port sends a character before the session is established, the port will discard the data. (If you enable LOSS NOTIFICATION. The port also sends the BELL character to the device.) This is the default setting.
ENABLED	The port will store data in its typeahead buffer while waiting for a session connection to be made, and then pass the data to the connection partner after the session connection is made. Typically, you will enable NOLOSS when the serial port is connected to a device that will begin sending data immediately after it issues a connect command. Use the TYPEAHEAD command to specify the maximum amount of data stored. If enabled, the port can accept input data when DCD/DSR is not asserted and modem control is enabled on the port.

Example

```
DEFINE PORT 5 NOLOSS DISABLED
```

DEFINE/SET PORT OUTBOUNDSECURITY Privilege: P

Use this command to enable the Kerberos, SECURID, RADIUS or simple port password security features on remote or dynamic ports. Without this feature, these security mechanisms do not apply to remote or dynamic ports.

Syntax

```
DEFINE/SET PORT [port-list] OUTBOUNDSECURITY     [ENABLED]
                                                 [DISABLED]
```

Where	Means
ENABLED	You can use Kerberos, SECURID, RADIUS or simple port password security features on the remote or dynamic port.
DISABLED	You cannot use Kerberos, SECURID, RADIUS or simple port password security features on the remote or dynamic port. This is the default setting.

Example

```
DEFINE PORT 5 OUTBOUNDSECURITY ENABLED
```

See Also

DEFINE/SET PORT KERBEROS
DEFINE/SET PORT SECURID
DEFINE/SET PORT RADIUS
DEFINE/SET PORT RADIUS PASSWORD

DEFINE/SET PORT OUTPUT FLOW CONTROL Privilege: N, P

Use this command to specify whether or not flow control will be used for output data communications at the port (i.e., data communication which originates at the server and is received by the device connected to the port). The flow control method used by the port (e.g., XON/XOFF, DCD/DTR, etc) is specified by the DEFINE/SET PORT FLOW command.

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list OUTPUT FLOW CONTROL  [DISABLED]
                                               [ENABLED]
```

Where	Means
DISABLED	The server port will not use flow control for output data communications.
ENABLED	The server port will use flow control for output data communications. This is the default.

Example

```
DEFINE PORT 5 OUTPUT FLOW CONTROL ENABLED
```

DEFINE/SET PORT PARITY — Privilege: N, P

Use this command to specify whether or not the port will provide a bit (parity bit) with each character for error checking. The value you set for this characteristic must match the value set at the device attached to the port.

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list PARITY    [EVEN]
                                    [MARK]
                                    [NONE]
                                    [ODD]
                                    [SPACE]
```

Where	Means
EVEN	The port will ensure that each byte (character) that is transmitted or received contains an even number of 1's, including the parity bit. If the port receives a byte that contains an odd number of 1 bits, it indicates to the server that an error occurred.
MARK	The port will always set the parity bit to 1. In this case, the device attached to the port needs to use the parity bit to mark the limit of each frame.
NONE	The port will not include a parity bit for error checking. This is the default value for the PARITY characteristic.
ODD	The port will ensure that each byte (character) that is transmitted or received contains an odd number of 1's, including the parity bit. If the port receives a byte that contains an even number of 1 bits, it indicates to the server that an error occurred.

Example

```
DEFINE PORT 5 PARITY ODD
```

DEFINE PORT PASSWORD — Privilege: P

Use this command to specify whether or not the user will be required to supply a password in order to logon to the port(s) listed in the port-list or all ports. If there will be ports that users will need to supply a password in order to logon, use the DEFINE/SET SERVER LOGIN PASSWORD command to specify the password.

This setting can only be changed with a DEFINE command, and also does not apply to parallel ports. A non-privileged user at one port cannot use a SETP PORT PPP command to enable PPP on another port.

Note: *See OUTBOUNDSECURITY for remote and dynamic ports.*

Syntax

```
DEFINE/SET PORT port-list  PASSWORD [DISABLED]
                                    [ENABLED]
```

Where	Means
DISABLED	Specifies that users will not be required to supply a password in order to logon to the port(s) listed in the port-list or all ports. This is the default setting.
ENABLED	Specifies that users will be required to supply a password in order to logon to the port(s) listed in the port-list or all ports.

Example

```
DEFINE PORT 5 PASSWORD ENABLED
```

DEFINE/SET PORT PASSWORD PROMPT Privilege: P

Use this command to define the prompt you want the users to see at login.

Syntax

```
DEFINE/SET PORT [port-list] PASSWORD PROMPT "string"
```

Where	Means
port-list	The port(s) that will display this prompt when a user logs on.
string	The login prompt that will display at user login. The prompt can be from 1 to 27 characters.Enclose the text in quotes (").

Example

```
DEFINE PORT PASSWORD PROMPT "Privileged Users"
```

DEFINE/SET PORT PAUSE — Privilege: N

Use this command to specify whether the device(s), attached to the port(s) listed in the port-list or all ports, will show server displays one screenful at a time (actually 24 lines at a time) or as a continuous stream of information. If these displays are shown one screenful at a time, the server will pause at the end of each screenful of information, and wait for the user to press a key before it displays the next screenful of information.

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list PAUSE  [DISABLED]
                                 [ENABLED]
```

Where	Means
DISABLED	The device(s), attached to the port(s) listed in the port-list or all ports, will show server displays as a continuous stream of information, rather than pausing at the end of each screenful of information. This is the default setting.
ENABLED	The device(s), attached to the port(s) listed in the port-list or all ports, will show server displays one screenful at a time, by pausing to wait for the user to press a key before it displays the next screenful of information.

Example

```
DEFINE PORT 5 PAUSE ENABLED
```

DEFINE/SET PORT PPP — Privilege: N, P

Use the Port PPP commands to specify which ports are used for PPP sessions.

A port that is configured as a PPP port can only be used for PPP sessions; i.e., only PPP packets can be sent or received by the port. A user at one port cannot use a SET PORT PPP command to enable PPP on another port.

Notes: *You can also use the SET PORT PPP ENABLED command while the port is in APD Interactive mode. This lets you set the protocol PPP, SLIP and ARAP on a port configured for APD after the port is in APD Interactive. Once the port is in APD Interactive the APD feature becomes disabled for that session and the Set command can be used to enable a protocol. Once the port is logged out, the APD feature is re-enabled.*

You cannot use the DEFINE PORT PPP or SLIP on a port that is in local access and has Kerberos or SecurID enabled. However, you can use the SET PORT PPP command to enable PPP.

Privilege

Non-privileged for your port. Privileged for other ports.

Syntax

```
DEFINE/SET PORT PPP port-list [DISABLED]
                              [ENABLED]
```

Where	Means
ENABLED	Enable the PPP protocol on one or more access server ports.
DISABLED	Disable the PPP protocol on one or more access server ports.This is the default setting.

Example

This command specifies that port 5 will be used for PPP sessions.

```
DEFINE PORT 5 PPP ENABLED
```

DEFINE/SET PORT PPP ACTIVE Privilege: N

Use this command to specify how the port will negotiate PPP options when a PPP session is initiated.

When a PPP session is initiated, the port and the remote device negotiate the manner in which data are to be transferred during the PPP session. The access server port can either initiate the negotiation of PPP options or it can wait until the remote device initiates the negotiation of the options.

When the server port initiates the option negotiations, this is referred to as an "active" start. When the server port waits until the remote device initiates the negotiation of the options, this is referred to as a "passive" start.

A non-privileged user at one port cannot use a SET PORT PPP ACTIVE command to change the method of option negotiation used at another port.

Syntax

Privilege Users:

```
DEFINE/SET PORT port-list PPP ACTIVE   [DISABLED]
                                       [ENABLED]
```

Non-privileged Users:

```
SET PORT PPP ACTIVE ENABLED
```

Where	Means
ENABLED	Configure the server port to initiate PPP option negotiations (perform an active start). This is the default setting.
DISABLED	Configure the server port to wait until the remote device initiates the negotiation of the options (perform a passive start).

Example

This command specifies that port 5 will initiate the option negotiations at the beginning of a PPP session rather than wait for the remote device to initiate negotiations.

```
DEFINE PORT 5 PPP ACTIVE ENABLED
```

DEFINE/SET PORT PPP CHAP CHALLENGE TIMER Privilege: P

Use this command to define how long the server will wait before re-challenging a peer after connection. A value of "0" disables this feature.

See the Security Features section of the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE/SET PORT [port number] PPP CHAP CHALLENGE TIMER [minutes]
```

Where	Means
minutes	The number of minutes the server will wait before re-challenging. A value of 0 disables the timer.

Example

```
DEFINE PORT 5 PPP CHAP CHALLENGE TIMER 10
```

DEFINE/SET PORT PPP CHAP RADIUS Privilege: P

Use this command to set the specified port to PPP CHAP RADIUS authentication. When you log in to the specified port, access to the port occurs only if the characteristics returned from the RADIUS server are for PPP CHAP. You can also use this command to specify whether or not the port will require a password in order to form a connection.

See the Security Features section of the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE/SET PORT [port number] PPP CHAP RADIUS   [DISABLED]
                                                [ENABLED]
```

Where	Means
DISABLED	The remote device does not need to supply the login password.
ENABLED	The remote device must supply the login password.

Example

```
DEFINE PORT 5 PPP CHAP RADIUS ENABLED
```

DEFINE/SET PORT PPP CHARMAP Privilege: N, P

Use this command to specify which ASCII control characters the port will propose to use as control characters rather than as data during PPP option negotiations.

During a PPP session, you might need to use some ASCII control characters to control how data is transferred (for example, for flow control purposes) from one end of the connection to the other. Other control characters may be part of a normal data stream. If these control characters were sent "in the clear" they would confuse devices such as modems, etc. The PPP RFC provides a standard way of "encoding" these characters so that both the port and the remote device can determine when they have received a control character rather than data. Control characters are converted into a two-byte token at one end of the link and then converted at the other end of the link. (The first byte of the token is 7D. The second byte is calculated by adding 20 plus the hexadecimal value of the control character to be encoded. For example, to send an encoded null character, which has the hexadecimal value of 00, the port will send the sequence 7D 20.)

In order to distinguish how one or more control characters are to be interpreted, the port and the remote device negotiate a mutually acceptable "character map." There can be separate character maps for each direction in which data are transmitted.

A non-privileged user at one port cannot use a SET PORT PPP CHARMAP command to alter the configuration for another port.

Syntax

Privileged users:

```
DEFINE/SET PORT port-list PPP CHARMAP <character-mask>
```

Non-privileged Users:

```
SET PORT PPP CHARMAP <character-mask>
```

Where	Means

character-mask

The hexadecimal 32-bit value of a control character that the port will propose to use as a control character during a PPP session. The specific control characters to be encoded by the port or the remote device are subject to negotiation.

Valid values are 00000000 through ffffffff. Commonly used masks include:

Where	Means
00000000	No control characters will be encoded.
000a0000	The XON and XOFF control characters will be encoded. This is the default.
ffffffff	All control characters will be encoded.

To calculate a different mask, select the control characters that are to be encoded from the following table.

0		NUL	Null
1	^A	SOH	Start of Heading
2	^B	STX	Start of Text
3	^C	ETX	End of Text
4	^D	EOT	End of Transmission
5	^E	ENQ	Enquiry
6	^F	ACK	Acknowledge
7	^G	BEL	Bell
8	^H	BS	Backspace
9	^I	HT	Horizontal Tab
10	^J	LF	Line Feed
11	^K	VT	Vertical Tab
12	^L	FF	Fprm Feed
13	^M	CR	Carriage Return
14	^N	SO	Shift Out
15	^O	SI	Shift In

16	^P	DLE	Data Link Escape
17	^Q	DC1	Device Control 1 (XON)
18	^R	DC2	Device Control 2
19	^S	DC3	Device Control 3 (XOFF)
20	^T	DC4	Device Control 4
21	^U	NAK	Negative Acknowledge
22	^V	SYN	Synchronous Idle
23	^W	ETB	End of Transmission Block
24	^X	CAN	Cancel
25	^Y	EM	End of Medium
26	^Z	SUB	Substitute
27		ESC	Escape
28		FS	File Separator
29		GS	Group Separator
30		RS	Record Separator
31		US	Unit Separator

The mask consists of eight hexadecimal characters (numbers 0 through 9 and the letters a through f), each represents four of the possible control character options. The bit ordering is from right to left as shown in the following figure. Each group of four bits is then converted to the hexadecimal character used in the mask.

Example

```
DEFINE PORT 5 PPP CHARMAP FFFFFFFF
```

DEFINE/SET PORT PPP CONFIGURE LIMIT Privilege: N, P

Use this command to specify the maximum number of unanswered PPP option configuration request packets that the port will send, before the software concludes that the remote device is unable to respond. (See the DEFINE/SET PORT PPP RESTART TIMER command for a description of how the CONFIGURE LIMIT command is used during PPP option negotiations.) When the port has sent the number of option configuration request packets specified by the PORT PPP CONFIGURE LIMIT setting, it discontinues further attempts to negotiate PPP options and goes into a passive "listening" state.

A non-privileged user at one port cannot use a SET PORT PPP CONFIGURE LIMIT command to alter the configuration for another port.

Syntax

Privileged users:

DEFINE/SET PORT *port-list* PPP CONFIGURE LIMIT <*limit*>

Non-privileged users:

SET PORT PPP CONFIGURE LIMIT <*limit*>

Where	Means
limit	The maximum number of unanswered PPP option configuration request packets that the port will send before discontinuing further attempts to negotiate PPP options and going into a passive "listening" state. Valid values are: 0 (Infinite) This setting allows an access port to try forever to bring up a PPP connection by sending out Configure Requests. 2 - 10 The default is 10.

Example

This command specifies that port 5 will send up to 5 PPP option configuration request packets, before discontinuing further attempts to negotiate PPP options and going into a passive "listening" state.

```
DEFINE PORTS 5 PPP CONFIGURE LIMIT 5
```

DEFINE/SET PORT PPP DEFAULTS Privilege: N

Use this command to reset the PPP operational settings back to their default values.

This command applies only for the specified port or ports on which PPP is enabled, and does not affect whether or not PPP is enabled for a given port.

A non-privileged user at one port cannot use a SET PORT PPP DEFAULTS command to resets the PPP operational characteristics used at another port back to their default values.

Syntax

Privileged users:

DEFINE/SET PORT *port-list* PPP DEFAULTS [ENABLED]

Non-privileged users:

```
SET PORT PPP DEFAULTS [ENABLED]
```

Where	Means
ENABLED	Optional keyword.

Examples

This command specifies that ports 8 through 16 will have the PPP operational settings changed to their default values.

```
DEFINE PORTS 8-16 PPP DEFAULTS ENABLED
```

DEFINE/SET PORT PPP FAILURE LIMIT Privilege: N, P

Use this command to determine how persistent the port should be in negotiating a given PPP option.

During PPP option negotiation, the remote device may propose values for options that cannot be accepted by the Xyplex unit. When this occurs, the port will object to (NAK) the option and offer a different value. Sometimes, the remote device will object to that value, and will propose the option again with a different setting. If the option is still unacceptable, the port will again object to (NAK) the option. This continues until the specified failure limit is reached, at which point the port rejects all further attempts at negotiating the option.

A non-privileged user at one port cannot use a SET PORT PPP FAILURE LIMIT command to alter the configuration for another port.

Syntax

Privileged users:

```
DEFINE/SET PORT port-list PPP FAILURE LIMIT limit
```

Non-privileged users:

```
SET PORT PPP FAILURE LIMIT limit
```

Where	Means
limit	The maximum number of times the port will reject an unsupported option or an unacceptable value for a supported option before the port rejects further negotiation of the option. Valid values between 2 and 10 rejections. The default is 3.

Example

This command specifies that port 5 will reject an unsupported option or an unacceptable value for a supported option up to 5 times before the port rejects further negotiation of the option.

```
DEFINE PORTS 5 PPP FAILURE LIMIT 5
```

DEFINE/SET PORT PPP IP BROADCASTS Privilege: N, P

Use this command to determine whether or not a port will transmit IP broadcast packets over the link or discard broadcast packets received from the remote device.

Internet broadcast packets are typically packets that contain route or routing information, information to resolve an Internet address or domain name, or requests for such types of information. In some configurations, such as single node (dial-in PC), it may be useful to eliminate forwarding of these packets in order to improve link efficiency. When the PPP link is used as a gateway, or when you are running a domain-name resolver program, you will usually want to have these packets be forwarded over the link.

A non-privileged user at one port cannot use a SET PORT PPP IP BROADCASTS command to alter the configuration for another port.

Syntax

Privileged users:

```
DEFINE/SET PORT port-list PPP IP BROADCASTS  [ENABLED]
                                             [DISABLED]
```

Non-privileged users:

```
SET PORT PPP IP BROADCASTS   [ENABLED]
                             [DISABLED]
```

Where	Means
ENABLED	Permit IP broadcast packets to be transmitted over the PPP link, or allow the port to accept broadcast packets received from the remote device and forward them to the local area network. This is the default.
DISABLED	Do not forward IP broadcast packets over the link to the remote device and discard any broadcast packets received from the remote device.

Example

This command specifies that port 5 will transmit Internet broadcast packets over the PPP link, and allow the port to accept broadcast packets received from the remote device and forward them to the local area network.

```
DEFINE PORT 5 PPP IP BROADCAST ENABLED
```

DEFINE/SET PORT PPP IP LOCAL ADDRESS Privilege: P

Use this command to determine whether the port will have a user-specified IP address or if the port will use the Internet address of the access server.

Both the port (the local end of a PPP connection) and the remote device must each have an Internet address assigned to them for the purpose establishing a connection and forwarding data. The Internet address of the port is referred to as a local address.

A non-privileged user at one port cannot use this command to alter the configuration for another port.

Syntax

Privileged users:

```
DEFINE/SET PORT port-list PPP IP LOCAL ADDRESS <internet-address>
```

Non-privileged users:

```
SET PORT port-list PPP IP LOCAL ADDRESS <internet-address>
```

Where	Means
internet-address	A standard IP address (refer to the section describing common variables). The default is 0.0.0.0 (no Internet address). If no IP address is assigned to the port, the port will use the access server's IP address as the local address when the PPP connection is established.

Example

The following command specifies that port 5 will have the local Internet address of 140.179.211.5.

```
DEFINE PORT 5 PPP IP LOCAL ADDRESS 140.179.211.5
```

DEFINE/SET PORT PPP IP LOCAL ADDRESS RANGE Privilege: P

Use this command to specify a range of local IP addresses that the port will use to for establish a connection and forward data. The IP address of the port is referred to as a local address. Use the PORT PPP IP LOCAL ADDRESS command to assign a specific IP address to a port.

A non-privileged user at one port cannot use this command to alter the configuration for another port.

Syntax

DEFINE/SET PORT [*port-list*] PPP IP LOCAL ADDRESS RANGE <*0.0.0.0 - 255.255.255.255*.>

Where	Means
range	Set a range of local IP addresses. Valid values are 0.0.0.0 - 255.255.255.255. The default is 0.0.0.0

Example

The following command specifies that port 5 will use a range of IP addresses as the local IP address.

```
DEFINE PORT 5 PPP IP LOCAL ADDRESS RANGE 0.0.0.0 - 255.255.255.255
```

DEFINE/SET PORT PPP IP MASK Privilege: P

Use the following command to allow subnets of IP addresses from a PPP port to map to an IP address specified by the mask. Use the PPP REMOTE ADDRESS command in conjunction with this mask to allow the port to map to a range of IP addresses.

Use the SHOW PORT IP CHAR command to display the port's current IP MASK settings.

The IP MASK is AND'ed with the REMOTE ADDRESS defined on the SLIP port to determine which subnet is off the serial port.

Note: *Xyplex recommends that you use the default IP mask of 255.255.255.255. Other masks will cause the access server to ARP connection, which has strange and varied effects on the network. PPP mask in NOT the same as subnet mask.*

Syntax

```
DEFINE/SET PORT <port number> PPP IP MASK [mask]
```

Where	Means
MASK	This Keyword must be used in order to map IP addresses to the port.
mask	Specify the mask to map to the port. The default is 255.255.255.255.

Example

```
DEFINE PORT 3 PPP IP MASK 255.255.255.255
```

DEFINE/SET PORT PPP IP REMOTE ADDRESS Privilege: P, N

Use this command to determine whether or not a port is constrained to use a specific remote address.

Both the port (the local end of a PPP connection) and the remote device must have an Internet address assigned to them in order to establish a connection and forward data. Normally, when a remote device wishes to make a connection during option negotiations it will either state the specific remote address that it wishes to use or indicate that it wishes to have a remote address assigned to it by the port.

You can also choose to dedicate the server port to a device with a specific remote address. (If the remote device supplies a remote address that is different than the one specified by the PORT PPP IP REMOTE ADDRESS command, then the connection can be made, but any data sent by the remote device will not be acknowledged, so the connection is not a useful one.) If neither the remote device nor the access server port can supply a remote address, then the PPP connection cannot be formed. When the port supplies the remote address, because the remote device indicates during option negotiations that it wants the access server to assign the remote address, the remote device must accept the address supplied to it or a non-meaningful connection will result.

A non-privileged user at one port cannot use a SET PORT PPP IP REMOTE ADDRESS command to alter the configuration for another port.

Syntax

Privileged users:

```
DEFINE/SET PORT port-list PPP IP REMOTE ADDRESS <ip-address>
```

Non-privileged users:

```
SET PORT PPP IP REMOTE ADDRESS <ip-address>
```

Where	Means
internet-address	A standard Internet address. The default is 0.0.0.0 (no Internet address). If no Internet address is assigned to the port, the port will use the Internet address specified by the remote device as the remote address when the PPP connection is established. (If that device does not offer a remote address, a connection cannot be established.)

Example

```
DEFINE PORT 5 PPP IP REMOTE ADDRESS 140.179.211.5
```

DEFINE/SET PORT PPP IP REMOTE ADDRESS RANGE Privilege: P, N

Use this command to determine the range of remote addresses a port can use.

Both the port (the local end of a PPP connection) and the remote device must have an Internet address assigned to them in order to establish a connection and forward data. Normally, when a remote device wishes to make a connection during option negotiations it will either state the specific remote address that it wishes to use or indicate that it wishes to have a remote address assigned to it by the port.

A non-privileged user at one port cannot use this command to alter the configuration for another port.

Syntax

Privileged user:

```
DEFINE/SET PORT port-list PPP IP REMOTE ADDRESS RANGE <0.0.0.0 - 255.255.255.255>
```

Non-privileged user:

```
SET PORT PPP IP REMOTE ADDRESS RANGE <0.0.0.0 - 255.255.255.255>
```

Where	Means
internet-address	A standard Internet address. The default is 0.0.0.0 (no Internet address). If no Internet address is assigned to the port, the port will use the Internet address specified by the remote device as the remote address when the PPP connection is established. (If that device does not offer a remote address, a connection cannot be established.)
RANGE	Set a range of local IP addresses. Valid values are 0.0.0.0 - 255.255.255.255. The default is 0.0.0.0

Example

```
DEFINE PORT 5 PPP IP REMOTE ADDRESS RANGE 140.179.211.5 - 140.179.211.8

DEFINE PORT 5 PPP IP REMOTE ADDRESS 0.0.0.0
```

DEFINE/SET PORT PPP IP VJ COMPRESSION Privilege: N, P

Use this command to specify whether or not the port will try to negotiate the use of a data compression mechanism over a PPP link.

Data compression allows more data to be transferred over the link. One popular method of data compression used in TCP/IP networks is known as Van Jacobson (VJ) compression. Other compression methods are also available, but are not currently supported by the Xyplex access server. The use of the Van Jacobson compression method can result in significant bandwidth savings, which can be important when PPP connections are made over telephone lines or when a PPP link is very heavily used. Van Jacobson compression is very memory intensive, however (see the DEFINE/SET PORT PPP IP VJ COMPRESSION SLOTS command description). The use of Van Jacobson compression is negotiated during PPP options negotiation. Compression can be used in one direction only.

A non-privileged user at one port cannot use this command to alter the configuration for another port.

Syntax

Privileged users:

```
DEFINE/SET PORT port-list  PPP IP VJ COMPRESSION      [ENABLED]
                                                      [DISABLED]
```

Non-privileged users:

```
SET PORT port-list  PPP IP VJ COMPRESSION      [ENABLED]
                                               [DISABLED]
```

Where	Means
ENABLED	Allow the port to negotiate the use of Van Jacobson compression. This is the default.
DISABLED	Do not allow the port to negotiate the use of Van Jacobson compression.

Example

```
DEFINE PORT 5 PPP IP VJ COMPRESSION ENABLED
```

DEFINE/SET PORT PPP IP VJ COMPRESSION SLOTS Privilege: N, P

A PPP link can have a number of sessions (or slots), using higher-level protocols such as TCP/IP, operating across the link. This can happen, for example, when the PPP link is used in a gateway configuration that supports several users, or in a configuration where a single node (such as a dial-in PC) is connected to the port and the single node has several windows in use. When Van Jacobson compression is in use on the link, PPP usually requires that both sides of the link must specify how many slots will use compression. PPP also requires that each slot have a unique slot number or address. For a link which supports 16 slots, the slots are numbered 0 through 15.

During PPP option negotiation, the remote device may propose a value for the number of slots that will use compression. If the number of slots proposed is between 3 and 15, the port will accept the proposed number. If the number of slots proposed is more than 16, the port will object to (NAK) the option and offer the value specified by the PORT PPP IP VJ COMPRESSION SLOTS setting. Sometimes, the remote device will accept that number. Other times, the remote device will object to that value, and will propose the option again with a different number of slots. If the number is still unacceptable, the port will again object to (NAK) the option and again propose the number specified by this setting. This continues until the number of times specified by the PORT PPP FAILURE LIMIT command is reached, at which point the port rejects all further attempts at negotiating the option.

A non-privileged user at one port cannot use this command to alter the configuration for another port.

Syntax

Privileged users:

```
DEFINE/SET PORT port-list  PPP IP VJ COMPRESSION SLOTS <number>
```

Non-privileged users:

```
SET PORT port-list PPP IP VJ COMPRESSION SLOTS <number>
```

Where	Means
number	The number of slots that can use Van Jacobson data compression over a PPP link that the port will propose during PPP options negotiation, when a value larger than 16 is proposed by the remote device. Valid values are between 3 and 15 slots. The default is 3.

Example

This command specifies that port 5 will propose using Van Jacobson compression on 15 slots if the port objects to the number of slots proposed by the remote device.

```
DEFINE PORT 5 PPP IP VJ COMPRESSION SLOTS 15
```

DEFINE/SET PORT PPP IPX SAP [BROADCAST] Privilege: P

This command specifies whether or not the port will broadcast SAP information over the serial link to the remote partner, and if the information is broadcast, how much information the PORT will send.

In some network configurations, an access server operates as an asynchronous IPX router. Servers in an IPX network (e.g., file servers, print servers) advertise their services through Service Advertising Protocol (SAP) packets. IPX servers also answer requests by clients who are looking for their services. IPX routers are responsible for broadcasting SAP information to other IPX routers in the network, and functioning as a proxy for servers on other networks. Each IPX router maintains a table of SAP information that it has received from neighboring routers and servers.

There are several commands available that control SAP broadcast and storage information.

Syntax

```
DEFINE/SET PORT port-list [PPP] IPX SAP [BROADCAST]  [FULL]
                                                     [CHANGE]
                                                     [NONE]
```

Where	Means
FULL	The server will broadcast the entire contents of the SAP table.
CHANGE	The server will only broadcast new or changed SAP information. This is the default.
NONE	The server will not broadcast any SAP information.

Example

```
DEFINE PORT 5 IPX SAP BROADCAST FULL
```

DEFINE/SET PORT [PPP] IPX SAP [BROADCAST] DISCARD TIMEOUT Priv: P

Use this command to specify how long the server will keep SAP information that it receives over the serial link to the remote partner.

In some network configurations, an access server operates as an asynchronous IPX router. Servers in an IPX network (e.g., file servers, print servers) advertise their services through Service Advertising Protocol (SAP) packets. IPX servers also answer requests by clients who are looking for their services. IPX routers are responsible for broadcasting SAP information to other IPX routers in the network, and functioning as a proxy for servers on other networks. Each IPX router maintains a table of SAP information that it has received from neighboring routers and servers.

There are several commands available that control SAP broadcast and storage information.

Syntax

DEFINE/SET PORT *port-list* [PPP] IPX SAP [BROADCAST] DISCARD TIMEOUT *timer-multiple*

Where	Means
timer-multiple	Specifies how long the server keeps SAP information that it receives over the serial link to the remote partner. The timer-multiple that you specify is multiplied by the value specified for the DEFINE/SET SERVER IPX SAP [BROADCAST] TIMER time command. Valid values for timer-multiple are between 0 and 4294967295. The default is 3.

Example

```
DEFINE PORT 5 IPX SAP BROADCAST DISCARD TIMEOUT 5
```

DEFINE/SET PORT [PPP] IPX SAP [BROADCAST] TIMER Privilege: P

Use this command to specify how frequently the communication port will broadcast SAP information over the serial link to the remote partner.

In some network configurations, an access server operates as an asynchronous IPX router. Servers in an IPX network (e.g., file servers, print servers) advertise their services through Service Advertising Protocol (SAP) packets. IPX servers also answer requests by clients who are looking for their services. IPX routers are responsible for broadcasting SAP information to other IPX routers in the network, and functioning as a proxy for servers on other networks. Each IPX router maintains a table of SAP information that it has received from neighboring routers and servers.

There are several commands available that control SAP broadcast and storage information.

Syntax

```
DEFINE/SET PORT port-list [PPP] IPX SAP [BROADCAST] TIMER timer
```

Where	Means
timer	The frequency at which the access server will broadcast SAP information over the serial link to the remote partner. Valid values are between 0 and 4294967295 (seconds). The default interval is 60 seconds.

Example

```
DEFINE PORT 5 IPX SAP BROADCAST TIMER 60
```

DEFINE/SET PORT PPP KEEPALIVE TIMER Privilege: P

Use this command to set the time between the LCP echo requests to be sent.

Syntax

```
DEFINE/SET PORT <port-list> PPP KEEPALIVE TIMER <seconds>
                [ALL]
```

Where	Means
seconds	The number of seconds between LCP echo requests to be sent. The valid values are 0 - 65535 seconds. The default is 6 seconds.

Example

```
DEFINE PORT ALL PPP KEEPALIVE TIMER 6
```

DEFINE/SET PORT PPP KEEPALIVE TIMEOUT Privilege: P

Use this command to set how long the PPP link will wait for an LCP echo reply before closing the link.

Syntax

```
DEFINE PORT <port-list> PPP KEEPALIVE TIMEOUT <seconds>
```

Where	Means
port-list	List the ports that will use this keepalive timeout value
seconds	The number of seconds the PPP link will wait for a reply before closing the link. The valid values are 0 - 65535 seconds. The default is 6 seconds.

Example

```
DEFINE PORT 4,6,8 PPP KEEPALIVE TIMEOUT 10
```

DEFINE/SET PORT PPP LOGGING Privilege: P

Use this command to define the logging type for PPP, LCP, IPCP and IPXCP port negotiations that will be logged in the access server accounting log.

***Notes**: You cannot issue this command from a remote terminal.*

> *With logging enabled, a reply message string received that is greater than 97 characters (96 + NULL) causes the client server to crash. To correct this problem, restrict the reply message strings (defined in the user record) to 97 characters or disable logging on the client server.*

Prerequisites

Before you can define this setting, you must enable the following options. Use the SHOW/MONITOR SERVER ACCOUNTING command to display the current settings.

1. Enable Accounting. Use the DEFINE SERVER ACCOUNTING ENTRIES and change the 0 (which disables accounting) to any number between 1 and 1000 to indicate the number of lines displayed in the accounting log.

2. Enable Verbose accounting. Use the DEFINE/SET SERVER VERBOSE ACCOUNTING ENABLED command

3. Set Verbose Accounting Priority to 7. Use the DEFINE/SET SERVER VERBOSE PRIORITY 7 LOG FACILITY LOCAL 7 command.

4. After you specify the logging type (INTERPRETED, RAW or NONE, enable RADIUS logging. Use the DEFINE SERVER RADIUS LOGGING ENABLED command

Syntax

```
DEFINE PORT <port-list> PPP LOGGING [INTERPRETED]
                                    [RAW]
                                    [NONE]
```

Where	Means
INTERPRETED	The information logged will be interpreted instead of displaying raw data.
RAW	The information will be logged as raw data.
NONE	Prevents logging on the specified port(s).

Example

```
DEFINE  PORT 4 PPP LOGGING INTERPRETED
```

DEFINE/SET PORT PPP MAGIC NUMBER Privilege: N, P

Use this command to enable or disable the magic number feature. When enabled, the access server can then attempt to negotiate the LCP magic number option when it starts up a PPP link. This magic number feature is used to detect loops in the PPP link.

Syntax

```
DEFINE/SET PORT [port-list] PPP MAGIC NUMBER   [ENABLED]
                                               [DISABLED]
```

Where	Means
ENABLED	You can use the magic number feature.
DISABLED	You cannot use the magic number feature. This is the default.

Example

```
DEFINE PORT 5 PPP MAGIC NUMBER DISABLED
```

DEFINE/SET PORT PPP PAP Privilege: P

Use these commands to determine whether or not the remote device must supply a password in order to establish a PPP connection with the server port, for Kerberos or RADIUS authentication.

You can configure the port (the local end of a PPP connection) and the remote device to require that the other end of the connection provides a password prior to establishing a PPP connection and forwarding data. You can also configure a link so that a password is required in either direction, both directions, or no direction. The DEFINE/SET PORT PPP PAP commands only affect whether or not the port will require a password in order to form a connection.

Syntax

```
DEFINE/SET PORT port-list PPP PAP      [LOCAL]     [ENABLED]
                                       [KERBEROS]  [DISABLED]
                                       [RADIUS]
```

Where	Means
PAP LOCAL	The server will use the standard login password. For ports that require the remote device to supply a password, the standard login password is the password that the remote device must supply. Use the DEFINE/SET SERVER LOGIN PASSWORD command to specify the password. The factory default password is "ACCESS." If the remote device does not supply this password, the port terminates further connection activities.
KERBEROS	The server will use Kerberos for PPP PAP authentication requests. Servers can be configured to authenticate PPP connections requests via either Kerberos version 4 or 5. When this feature is enabled, the peer (the remote partner) sends a PAP authentication request packet, which contains a user identification and password. The server then passes these items to the Kerberos host for authentication, and permits or denies the connection request based upon the answer from the host. In order to use this feature, first configure Kerberos and PPP PAP, as described in the Security section of the *Advanced Configuration Guide*. After these activities are completed, you can use this command to enable Kerberos authentication for PPP PAP requests.
NOTE:	If a port is configured to use Kerberos authentication for PPP PAP authentication requests (i.e., DEFINE PORT PPP PAP is set to KERBEROS), but Kerberos authentication is disabled on the unit, then PPP PAP authentication will be performed using the non-Kerberos "standard" PPP PAP method. In this case, the login password will be used to authenticate the connection.

DEFINE/SET PORT PPP PAP (continued)

RADIUS	The server will use RADIUS for PPP PAP authentication requests. When you log in to the defined port, access to the port occurs only if the information returned from the RADIUS server is for PPP PAP.
ENABLED	The remote device must supply the login password in order to establish a PPP connection with the port.
DISABLED	The remote device does not need to supply the login password in order to establish a PPP connection with the port. This is the default.

Examples

```
DEFINE PORT 5 PPP PAP RADIUS

DEFINE PORTS 8-16 PPP PAP ENABLED
```

DEFINE/SET PORT PPP RESTART TIMER Privilege: N, P

Use this command to specify how many seconds the port should wait after sending a configuration request to the remote device before sending another configuration request.

When a PPP session is initiated, the port and the remote device negotiate how the data will be transferred during the PPP session. Each partner on the link sends an initial configuration request packet to the other to start these option negotiations. If, after sending its configuration request packet, the access server port has not received a response from the remote device within the time specified by the RESTART TIMER setting, the port sends another option configuration request. This continues until the number of retries specified by the PORT CONFIGURE LIMIT setting is reached, at which time the port assumes that the remote device is no longer available and goes into a passive "listening" state.

This setting applies to ports that actively start option negotiations as well as ports that wait for the remote device to start the option negotiations.

A non-privileged user at one port cannot use a SET PORT PPP RESTART TIMER command to alter the configuration for another port.

Syntax

Privileged users:

```
DEFINE/SET PORT port-list  PPP RESTART TIMER <time>
```

Non-privileged users:

```
SET PORT port-list  PPP RESTART TIMER <time>
```

Where	Means
RESTART	Optional keyword.
time	How many seconds the port should wait before sending another option configuration request packet. Valid values for *time* are 1 to 10 seconds. The default is 3 seconds.

Examples

```
DEFINE PORTS 5 PPP RESTART TIMER 5
```

DEFINE/SET PORT PREFERRED SERVICE Privilege: N

Use this command to specify if there will be a service to which the port will connect whenever a user makes a connect request without specifying a service. It can also be used to change the current preferred service assignment for the port.

When a connection is attempted, the server will interpret the service information as either a LAT service-name or as a Telnet destination (domain-name or internet-address), depending on the RESOLVE SERVICE setting. You can also specify the prefixes LAT or TELNET to require the server to interpret the variable as a LAT service-name or a Telnet destination. (See the RESOLVE SERVICE, LAT and TELNET PREFERRED SERVICE commands for more information.)

Note: *When you define a port for preferred service the user will still be able to access the Xyplex prompt when disconnected from the preferred host. When you define a port as Dedicated Service the user will not see the prompt when disconnected.*

Syntax

DEFINE/SET PORT *port-list* PREFERRED SERVICE *service-information*

where the following is the syntax for *service-information*:

```
[service-name][NODE] [node name]    [DESTINATION]     [port name] [CONTROLLED]
                                    [NONE]

                     [NONE]         [DESTINATION]     [port name]
                                                      [NONE]
                                    [NONE]            [NODE][node name]
                     [DESTINATION][port name]
                     [NONE]
                                    [NONE]      [DESTINATION]     [port name]
                                                [NONE]
                     [domain-name[:telnet-port number]]
                     [internet-address[:telnet-port number]]
```

DEFINE/SET PORT PREFERRED SERVICE (continued)

Where	Means
service-name	The name of a LAT service to which the port is automatically connected when a user makes a connect request without specifying a service-name.
NODE	Indicates that you will set or change the name of the node where the preferred service is offered. (This keyword only applies to services that are offered on a LAT network.)
node name	The name of the service node where the preferred service is offered.
DESTINATION	Indicates that you will set or change the name of the server port that offers the preferred service. (This keyword only applies to services that are offered on a LAT network.)
port name	The name of the server port at which the service, specified by the service-name, is offered.
NONE	Indicates that this port, all ports, or the ports listed in the port-list will not have a preferred service, or that you wish to cancel a previously-defined preferred service, service node, or destination server port. This is the default setting for PREFERRED SERVICE, NODE, and DESTINATION.
domain-name	The logical name of the Telnet destination to which the port will be connected, whenever a user makes a connect request without specifying a domain-name. If the specified *domain-name* is not a fully qualified domain-name, the specified name will be concatenated with the default IP domain-name-suffix.
internet-address	The IP address of the Telnet destination on the network where the port will be connected whenever a user makes a connect request without specifying an internet-address.
:telnet-port number	The number of the target Internet protocol or physical port address which will be used for sessions between the port and the Telnet destination to which the port will be connected, whenever a user makes a connect request without specifying a Telnet addressable network object. Note that a colon is used before the Telnet port number
CONTROLLED	The connection will use the strings defined with the DEFINE/SET PORT CONTROLLED SESSION command.

Example

```
DEFINE PORT 5 PREFERRED SERVICE FINANCEVAX

DEFINE PORT 5 PREFERRED SERVICE FINANCEHOST.XYPLEX.COM

DEFINE PORT 5 PREFERRED SERVICE 140.179.249.100
```

DEFINE/SET PORT PRIVILEGED MENU Privilege: P

Use this command to specify which ports will have the menu feature enabled and which will be privileged when the user logs on. The PORT MENU must also be ENABLED for the port.

If you disable this feature at a port where both the MENU feature and the PRIVILEGED MENU feature are enabled, the server will disable both menu features. You can re-enable the regular menu with the DEFINE/SET PORT MENU ENABLED command.

Syntax

```
DEFINE/SET PORT port-list PRIVILEGED MENU   [DISABLED]
                                            [ENABLED]
```

Where	Means
DISABLED	The port(s) where the menu feature is enabled will not be privileged when the user logs on. This is the default setting.
ENABLED	The port(s) will have the the menu feature enabled and will be privileged when a user logs on.

Example

```
DEFINE PORT 5 PRIVILEGED MENU ENABLED
```

DEFINE/SET PORT PRIVILEGED NESTED MENU Privilege: P

This command allows you to include privileged commands in nested menus without explicitly setting the privileged security level within the menu script.

When you disable the Privileged Nested Menu feature at a port, you also disable the Nested Menu Feature at the port.

If you do not enable this feature, and you want to include a privileged command in a menu, you need to include the SET PRIVILEGE command within the menu script.

If the access server cannot access the menu file, and the Privileged Nested Menu feature is enabled at a port, the security level of the port is Nonprivileged when the user logs in to the Xyplex command interface.

Syntax

```
DEFINE/SET PORT port-list PRIVILEGED NESTED MENU   [ENABLED]
                                                   [DISABLED]
```

Where	Means
port-list	One or more ports where you want to specify the status of the Privileged Nested Menu feature.
ENABLED	Enable Privileged Nested Menus at the ports you specify.
DISABLED	Disable Privileged Nested Menus at the ports you specify. This is the default setting.

Example

This command enables Privileged Nested Menus on ports 10-20.

```
SET PORT 10-20 PRIVILEGED NESTED MENU ENABLED
```

DEFINE/SET PORT PROMPT Privilege: N, P

Use this command to change the prompt which is displayed at the devices connected to the server serial port(s).

A non-privileged user at one port cannot use a SET PORT PROMPT command to alter the configuration on another port.

Syntax

Privileged users:

`DEFINE/SET PORT` *`port-list`* `PROMPT` *`"prompt"`*

Non-privileged users:

`SET PORT` *`port-list`* `PROMPT` *`"prompt"`*

Where	Means
"prompt"	Display this prompt at the devices connected to the server port(s). The prompt can be between 1 - 20 characters. Always enclose the prompt text string in quotation marks ("). The prompt "Xyplex" is the default setting.

Example

```
SET PORT PROMPT "John"

John>>
```

DEFINE/SET PORT QUEUING Privilege: P

Use this command to specify whether or not the port(s) can place a connection request into a queue (called a connection queue) when the requested service is busy.

Service requests that are in the connection queue, when queuing is enabled at a port, stay in the connection queue until the service becomes available.

Use this setting when LAT local services are offered at the port.

Syntax

```
DEFINE/SET PORT port-list QUEUING   [DISABLED]
                                    [ENABLED]
```

Where	Means
DISABLED	The port(s) will not place a connection request into a connection queue when the requested service is busy. This is the default setting.
ENABLED	The port(s) can place a connection request into a connection queue when the requested service is busy.

Example

```
DEFINE PORT 5 QUEUING ENABLED
```

DEFINE/SET PORT RADIUS Privilege: P

Use this command to enable the Radius authentication feature on a particular access server port. You can enable each port separately.

See Security Features in the *Advanced Configuration Guide* for more information. See the OUTBOUNDSECURITY command for ports configured as dynamic or remote.

Syntax

```
DEFINE/SET PORT [port number] RADIUS      [ENABLED]
                                          [DISABLED]
```

Where	Means
port number	The port number you are enabling for Radius.
ENABLED	You can use the Radius authentication feature on the specified access server port.
DISABLED	The specified port will not use Radius authentication.

Example

```
DEFINE PORT 5 RADIUS ENABLED
```

DEFINE/SET PORT RADIUS ACCOUNTING Privilege: P

Use this command to enable the Radius Accounting feature on a defined access server port. You can enable each port separately.

Syntax

```
DEFINE/SET PORT [port number] RADIUS   [ACCOUNTING]   [ENABLED]
                                                     [DISABLED]
                                                     [LIMITED]
```

Where	Means
port number	The port number you are enabling for Radius.
ACCOUNTING	Enables Radius Accounting on the specified port.
ENABLED	You can use the Radius authentication feature on the specified access server port.
DISABLED	The specified port will not use Radius authentication.
LIMITED	Provide only basic accounting information.

Example

```
DEFINE PORT 5 RADIUS ACCOUNTING ENABLED
```

DEFINE/SET PORT RADIUS SOLICITS Privilege: P

Use this command to enable the Radius authentication service solicitation feature on a defined access server port. You can enable each port separately to use the Radius solicitation feature.

Syntax

```
DEFINE/SET PORT [port number] RADIUS SOLICITS[ENABLED]
                                             [DISABLED]
```

Where	Means
ENABLED	You can use the Radius authentication solicitation feature on the specified access server port.
DISABLED	You cannot use the Radius authentication solicitation feature on the specified access server port.

Example

```
DEFINE PORT 5 RADIUS SOLICITS ENABLED
```

DEFINE/SET PORT REMOTE DISCONNECT NOTIFICATION Privilege: P

Use this command to control sending of warning (BEL) out serial port upon network session disconnect from port with remote access.

Syntax

```
DEFINE/SET PORT REMOTE DISCONNECT NOTIFICATION  [ENABLED]

                                                [DISABLED]
```

Where	Means
ENABLED	The serial port will receive a notification if a network session is disconnected.
DISABLED	No notification will be issued if a network session is disconnected.

Example

```
DEFINE PORT [port-list] REMOTE DISCONNECT NOTIFICATION ENABLED
```

DEFINE/SET PORT REMOTE MODIFICATION Privilege: P

Use this command to specify whether or not a process running at a VMS host can change certain PORT settings. You can change the following PORT settings: CHARACTER SIZE, INPUT SPEED and OUTPUT SPEED, LOSS NOTIFICATION, and DEFAULT SESSION MODE.

Refer to the documentation supplied with your VMS application to determine whether or not you should enable this feature.

Syntax

```
DEFINE/SET PORT [port-list]  REMOTE MODIFICATION   [ENABLED]
                                                   [DISABLED]
```

Where	Means
ENABLED	Specifies that a process running at a VMS host can change certain port settings.
DISABLED	Specifies that a process running at a VMS host cannot change certain port settings. This is the default.

Example

```
DEFINE PORT 5 REMOTE MODIFICATION ENABLED
```

DEFINE/SET PORT RESOLVE SERVICES Privilege: S, N, P

Use this command to specify whether the server should interpret the variable specified in a user CONNECT, SET PORT PREFERRED SERVICE, or SET PORT DEDICATED SERVICE command as a LAT service-name or as a Telnet destination. (This setting does not apply when the keywords LAT or TELNET are used.)

This applies to connections from and to a port. If you attempt to connect to a target port that has RESOLVE SERVICES set to a specific protocol (LAT or Telnet), from a port whose RESOLVE SERVICES is not set to the same protocol, the server does not allow the connection.

Syntax

```
DEFINE/SET PORT port-list RESOLVE SERVICES      [ANY]
                                                [LAT]
                                                [TELNET]
                                                [ANY_LAT]
                                                [ANY_TELNET]
```

Where	Means
ANY	The server tries to interpret the variable, specified in a CONNECT, SET PORT PREFERRED SERVICE or SET PORT DEDICATED SERVICE command, as a LAT service-name. If the server cannot connect to a matching LAT service, it then tries to connect to a TELNET destination (domain-name or internet-address).
LAT	The server interprets the variable, specified in CONNECT, SET PORT PREFERRED SERVICE or SET PORT DEDICATED SERVICE commands, as a LAT service name.
TELNET	The server interprets the variable specified in CONNECT, SET PORT PREFERRED SERVICE or SET PORT DEDICATED SERVICE commands, as a Telnet destination.
ANY_LAT	The server first tries to resolve the name as a LAT service name. If that fails, the server then resolves it as a TELNET domain name. This is the default setting.
ANY_TELNET	The server first tries to resolve the name as a TELNET domain name. If that fails, the server then resolve it as a LAT service name.

Example

```
DEFINE PORT 5 RESOLVE SERVICES ANY
```

DEFINE/SET PORT RLOGIN DEDICATED SERVICE Privilege: P

Use this command to enable a dedicated service using RLOGIN. Use the SHOW PORT *port number* command to display the port's current dedicated services.

Notes: *With dedicated RLOGIN service, you cannot specify a different username for RLOGIN. the only valid username is the port's username.*

When you define a port for dedicated service the user will not be able to access the Xyplex prompt when disconnected from the preferred host. When you define a port as preferred service the user will see the prompt when disconnected

Syntax

DEFINE PORT *port-list* RLOGIN DEDICATED SERVICE *service-name*

Where	Means
port-list	The specified port will use RLOGIN as a dedicated service.
DEDICATED SERVICE	The port will connect only to the service specified.
service-name	The name or IP address of the dedicated service.

Example

```
DEFINE PORT 4 RLOGIN DEDICATED SERVICE 140.179.111.66
```

DEFINE/SET PORT RLOGIN PREFERRED SERVICE Privilege: P

Use this command to enable a preferred service using RLOGIN. Use the SHOW PORT command to display the current preferred service setting for the port

Notes: *With preferred RLOGIN service, you cannot specify a different username for RLOGIN. The only valid username is the port's username.*

When you define a port for dedicated service, the user will not be able to access the Xyplex prompt when disconnected from the preferred host. When you define a port for preferred service the user will see the prompt when disconnected.

Syntax

```
DEFINE PORT port-list RLOGIN PREFERRED SERVICE service-name
```

Where	Means
port-list	The specified port will use RLOGIN as a preferred service.
PREFERRED SERVICES	The port will connect only to the service specified.
service-name	The name or IP address of the preferred service.

Example

```
DEFINE PORT 4 RLOGIN PREFERRED SERVICE 140.179.111.66
```

DEFINE/SET PORT RLOGIN TRANSPARENT MODE Privilege: P

Use this command to enable the access server to complete a ZMODEM transfer using the RLOGIN feature.

Syntax

```
DEFINE/SET PORT [port number] RLOGIN TRANSPARENT MODE [ENABLED]
                                                      [DISABLED]
```

Where	Means
port number	The number of the port.
ENABLED	Within an RLOGIN session, characters are passed *raw* (without interpretation) and transparently. This allows the ZMODEM transfer to complete.
DISABLED	RLOGIN operates in normal mode. This is the default setting.

ZModem Requirements

Feature	Setting
Typeahead	1024
TCP Window Size	1024
Telnet CSI ESC	Enabled
Telnet NEW LINE FILTER	LF or Standard

Example

```
DEFINE PORT 5 RLOGIN TRANSPARENT MODE ENABLED
```

SET PORT SCRIPT — Privilege: N, P

Use this command to have the port download a script from a script server and perform the commands contained in the script file.

Refer to the Scripts section of the *Advanced Configuration Guide* for more information about using scripts.

You can substitute the SCRIPT command as a shortcut for the SET PORT SCRIPT command.

Syntax

```
[SET PORT] SCRIPT "script-pathname"

SCRIPT "script-pathname"
```

Where	Means
SET PORT	Optional keywords.
"script-pathname"	The name and directory location of the script file to be executed, specified by a UNIX-style pathname, for example: */usr/login*). You must enclose the *script-pathname* in quotation marks ("). The maximum length of the script pathname is 64 characters. If you do not specify a script pathname, the server tries to execute the script file that is normally executed when the user logs on to the port.

Example

```
SET PORT SCRIPT "/usr/login"
```

DEFINE/SET PORT SCRIPT ECHO Privilege: P

Use this command to specify whether or not the port will display the TCP/IP-LAT commands contained in a script file while they are being executed.

See the Scripts section of the *Advanced Configuration Guide* for more information about using scripts.

Syntax

```
DEFINE/SET PORT port-list SCRIPT ECHO  [DISABLED]
                                       [ENABLED]
```

Where	Means
DISABLED	The port will not display the TCP/IP-LAT commands contained in a script file while they are being executed. This is the default.
ENABLED	The port will display the TCP/IP-LAT commands contained in a script file while they are being executed.

Example

```
DEFINE/SET PORT 5 SCRIPT ECHO ENABLED
```

DEFINE PORT SCRIPT LOGIN Privilege: P

Use this command to specify whether or not the port(s) will require a login script file to be downloaded from a script server and then executed, in order to complete the login sequence.

See the Scripts section of the *Advanced Configuration Guide* for more information about using scripts.

Syntax

```
DEFINE/SET PORT port-list SCRIPT LOGIN    [DISABLED]
                                          [ENABLED]
                                          [REQUIRED]
```

Where	Means
DISABLED	The port(s) do not need to have a login script file downloaded from a script server and then executed, in order to complete the login sequence. This is the default.
ENABLED	The port(s) will request that a login script file be downloaded from a script server and then executed, prior to completing the login sequence. The port is logged on, even if the server is unable to locate a script file.
REQUIRED	The port(s) require a login script file to be downloaded from a script server and then executed, in order to complete the login sequence. If the server is unable to locate the correct script file, the port is logged out.

Example

```
DEFINE PORT 5 SCRIPT LOGIN REQUIRED
```

DEFINE PORT SECURID — Privilege: P

Use this command to specify which ports will require SecurID authentication for the user to gain access to the port.

The SecurID feature must first be enabled on the server using the DEFINE SERVER SECURID ENABLED command, and other server settings must have been configured appropriately. See the Security Features section of the *Advanced Configuration Guide* for more information about setting up the SecurID feature. Also refer to the OUTBOUNDSECURITY command for ports configured as remote or dynamic.

Note: *The SET command is not available for this feature.*

Syntax

```
DEFINE/SET PORT [port-list] SECURID [ENABLED]
                                    [DISABLED]
```

Where	Means
port-list	One or more ports where you want to specify the status of the SecurID feature.
ENABLED	Enable SecurID at the ports you specify. The ports in the *port-list* will require that the SecurID authenticate the user when he or she logs in.
DISABLED	Disable SecurID at the ports you specify. This is the default.

Example

```
DEFINE PORT 10-20 SECURID ENABLED
```

DEFINE/SET PORT SECURITY Privilege: P

Use this command to specify whether or not the port(s) listed in the port-list or all ports will be set to the Secure privilege level. Ports that are set to Secure status are restricted from having access to some port configuration commands and from using the SHOW command to view information about other user's ports or sessions. See the Security Features section of the *Advanced Configuration Guide* for more information about port security levels.

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list SECURITY  [DISABLED]
                                    [ENABLED]
```

Where	Means
DISABLED	The port(s) listed in the port-list or all ports will not be set to secure status. This is the default setting.
ENABLED	The port(s) listed in the port-list or all ports will be set to secure status.

Example

```
DEFINE PORT 5 SECURITY ENABLED
```

SET PORT SESSION MODE Privilege: P

Use this command to define the default session mode. You cannot modify this setting with the DEFINE command.

Use the SHOW/LIST PORT CHARACTERISTICS command to display the port's current session setting.

Syntax

```
SET PORT SESSION        [INTERACTIVE]
                        [INTERACTIVE_NOIAC]
                        [PASTHRU]
                        [LIMIT]
                        [PASSALL]
                        [TRANSPARENT]
```

Where	Means
INTERACTIVE	The server will initially set all sessions so that all switching characters, Telnet command characters, and XON/XOFF flow control recognition are enabled. The server will not attempt to negotiate the TELNET binary option. This is the default.
INTERACTIVE_NOIAC	The server will act like it is in Interactive mode, but does not process or send any Telnet options.
PASTHRU	The server will initially set all sessions so that all switching characters and Telnet command characters are interpreted as data, but XON/XOFF flow control is still used in this mode. The server will attempt to negotiate the TELNET binary option.
PASSALL	The server will initially set all sessions so that all switching characters, Telnet command characters, and XON/XOFF flow control recognition are disabled. The server will attempt to negotiate the TELNET binary option.
TRANSPARENT	The server will initially set all sessions so that a Telnet session will ignore Telnet option messages received from a remotely initiated session and will not send any Telnet option messages from the locally initiated session, in addition to disabling all switching characters, Telnet command characters, and XON/XOFF flow control recognition. For a LAT session, the server tells its partner it is PASSALL but acts locally as if it were PASTHRU.

DEFINE/SET PORT SESSION LIMIT — Privilege: P

Use this command to change the maximum number of sessions that can be simultaneously established on any given port. Additional sessions can require additional server resources. The number of sessions that are permitted varies, depending on the product and type of port. Refer to the Server Settings section in the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE/SET PORT port-list SESSION LIMIT   [session-limit]
                                          [NONE]
```

Where	Means
session-limit	The maximum number of sessions that can be simultaneously connected to the port(s) specified by the port-list. The number of sessions that are permitted varies depending on the product and type of port. For most products, valid values are between 0 and 16. The default value is 4.
NONE	The server port(s) specified by the *port-list* can be simultaneously connected to as many sessions as memory will permit.

Example

```
DEFINE PORT 5 SESSION LIMIT 8
```

DEFINE/SET PORT SIGNAL CHECK Privilege: P

Use this command to restrict connections to a service offered at this port, if the DSR signal is deasserted. Also specifies whether or not the server should log out a port when the DCD signal is deasserted. The SIGNAL CHECK setting only applies for ports where FLOW CONTROL is set to any value except CTS or DSR, and only applies to serial ports that support modem signals. This command does not apply to parallel ports.

See the Modems section of the *Basic Configuraton Guide* for more information.

Syntax

```
DEFINE/SET PORT port-list  SIGNAL [CHECK] [ENABLED]
                                          [DISABLED]
```

Where	Means
CHECK	An optional keyword that restricts connections to a service defined on a server if the DSR signal is not asserted.
DISABLED	Allow connections to a service offered at the port when DSR is deasserted. Do not logout appropriately configured ports when the serial interface DCD signal is deasserted. This is the default setting.
ENABLED	Disallow connections to a service offered at the port when DSR is deasserted. Logout appropriately configured ports when the serial interface DCD signal is deasserted.

Example

```
DEFINE PORT 5 SIGNAL CHECK ENABLED
```

DEFINE/SET PORT SLIP IP MASK Privilege: P

Use the following command to allow subnets of IP addresses from a SLIP port to map to a range of Internet addresses specified by the mask. Use the PPP REMOTE ADDRESS command in conjunction with this mask to allow the port to map to a range of IP addresses.

Use the SHOW PORT IP CHAR command to display the port's current IP MASK settings.

The IP MASK is AND'ed with the REMOTE ADDRESS defined on the SLIP port to determine what subnet is off the serial port.

Syntax

DEFINE PORT <*port number*> SLIP IP MASK [*mask*]

Where	Means
MASK	This Keyword must be used in order to map an IP address to the port.
mask	Specify the mask to map to the port.

Example

```
DEFINE PORT 3 SLIP IP MASK 255.255.255.255
```

DEFINE/SET PORT SPEED Privilege: N, P

Use the DEFINE/SET PORT SPEED command to set or change the port speed (baud rate) for one or more ports to match the speed of the device connected to the port.The server will also use this setting when negotiating options for TELNET and RLOGIN connections.

Note: *Split speed operation (i.e., input speed different from output speed) is not supported. Not all servers support speeds above 38,400 bps.*

A non-privileged user at one port cannot use this command to alter the configuration of another port.

See also DEFINE/SET PORT INPUT SPEED and DEFINE/SET PORT OUTPUT SPEED commands.

This setting does not apply to parallel ports.

Privilege

Non-privileged for your own port. Privileged for other ports.

Syntax

`DEFINE/SET PORT` *`port-list`* `SPEED` *`speed`*

Where	Means
speed	The port speed, in bits per second, to which the specified port(s) will be set. Valid speeds are 50, 75, 110, 134, 150, 300, 600, 1200, 1800, 2000, 2400, 4800, 9600, 14400, 19200, 21600, 26400, 28800, 33,600, 38400. Some servers also support the following speeds: 56000, 57600, 64000, 76800, and 115200.

Example

```
DEFINE PORT 5 SPEED 28800
```

DEFINE/SET PORT STOP BITS Privilege: P

Use this command to change the number of stop bits to be used to maintain synchronization of data.

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list  STOP BITS bit-value
```

Where	Means
bit-value	A whole number which maps to the number of stop bits to be used to maintain synchronization of data. The following table indicates how many stop bits will be used for various settings of the *bit-value*:

Bit-value Setting	Stop Bits Used
1	1 stop bit
2	2 stop bits
3	1.5 stop bits
4	Server calculates the number of stop bits to use based on the port speed. This is the default.

Example

```
DEFINE PORT 5 STOP BITS 3
```

DEFINE/SET PORT TELNET ABORT OUTPUT Privilege: S, N, P

Use this command to specify whether or not there will be a character, which the user can type during a Telnet session, which terminates the further display of output (such as a text file, etc) at a terminal. (However, typing this character does not abort or terminate any programs that are running - it merely terminates the display of the output of the program.)

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list TELNET ABORT OUTPUT  [character]
                                               [NONE]
```

Where	Means
character	The character which, when typed by a user during a Telnet session, terminates further display of output at a terminal. It is recommended that you specify an unused CTRL character for this setting. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, with the character you set for the BACKWARD SWITCH, FORWARD SWITCH, or the LOCAL SWITCH settings, any line editing commands, or any other Telnet command characters). If your network supports both LAT and Telnet sessions, you may minimize user confusion caused by switching among different session types if you specify a VMS equivalent to the TELNET ABORT OUTPUT setting (in this case CTRL/O).
NONE	There will not be a character, which the user can type during a Telnet session, which terminates the display of output at a terminal. This is the default.

Example

```
DEFINE PORT 5 TELNET ABORT OUTPUT ^O
```

DEFINE/SET PORT TELNET ATTENTION Privilege: S, N, P

Use this command to specify whether or not there will be a character which, when typed by a user in a Telnet remote session, causes the Telnet host to return to the operating system command prompt. When a user issues the TELNET ATTENTION command, the remote server port will pass a BREAK to the host or device to which it is connected.

This setting does not apply to parallel ports. See also the DEFINE/SET PORT BREAK command.

Syntax

```
DEFINE/SET PORT port-list  TELNET ATTENTION  [character]
                                             [NONE]
```

Where	Means
character	The character which, when typed by a user in a Telnet session, causes the Telnet host to return to the operating system command prompt. It is recommended that you specify an unused CTRL character for this setting. Be sure that the character you select does not conflict with (particularly with control characters that are used by applications programs) the character you set for the BACKWARD SWITCH, FORWARD SWITCH, or the LOCAL SWITCH, line editing command, or any other Telnet command characters. If your network supports both LAT and Telnet sessions, you can minimize user confusion caused by switching among different session types if you specify a VMS equivalent to the TELNET ATTENTION setting (in this case CTRL/Y).
NONE	There will not be a character which, when typed by a user in a Telnet session, causes the Telnet host to return to the operating system command prompt. This is the default setting.

Example

```
DEFINE PORT 5 TELNET ATTENTION ^Y
```

DEFINE/SET PORT TELNET BINARY SESSION MODE Privilege: N, P

Use this command to specify whether or not Telnet sessions will negotiate binary mode, and for ports that can negotiate binary mode, if they should change their session mode to PASSALL or PASTHRU after they have negotiated binary mode.

The session mode (Passall or Pasthru) that will be used when the port negotiates the Telnet binary mode, or Interactive if the port should not negotiate the Telnet binary mode, Interactive_NOIAC (which acts like interactive but does not process or send any Telnet options).
This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list TELNET BINARY SESSION MODE    [INTERACTIVE]
                                                        [PASSALL]
                                                        [INTERACTIVE_NOIAC]
                                                        [PASTHRU]
```

Where	Means
INTERACTIVE	When binary negotiation is initiated from a remote host, the port will negotiate "won't binary".
PASSALL	The port(s) can negotiate binary mode, but disables all switch characters, Telnet command characters, server messages, and XON/XOFF flow control. In PASSALL mode, all characters are passed to the connection partner as data. This allows data files that contain control characters to be transferred without interference from the server. Typically, you would use this mode for binary file transfers (e.g., transferring a program via modem).
PASTHRU	The port(s) can negotiate binary mode, but disables all switch characters, Telnet command characters, server messages, but leaves XON/XOFF flow control enabled. Typically, you would use this mode for ASCII file transfers (e.g., printing on a line printer connected to a port). This is the default setting.
Interactive_NOIAC	The port acts like interactive but does not process or send any Telnet options).

Example

```
DEFINE PORT 5 TELNET BINARY SESSION MODE PASSALL
```

DEFINE PORT TELNET COMPORTCONTROL Privilege: P

Use this command to enable the use of RFC2217(Telnet Com Port Control Options) as described in this section. Use the SHOW/LIST PORT TELNET COMPORTCONTROL CHARACTERISTICS command to display the current settings.

Note: *There is no SET command for this feature. You must log out from the port before the changes can take effect.*

Syntax

```
DEFINE PORT port-list TELNET COMPORTCONTROL [CLIENT] [DISABLED]
                                            [SERVER] [ENABLED]

DEFINE PORT port-list TELNET COMPORTCONTROL[CLIENT TOGGLES DTR][DISABLED]
                                          [SERVER RAISES DTR] [ENABLED]
```

Command	Description
ENABLED	Enables any of these functions.
DISABLED	Disables COMPORTCONTROL. This is the default for all COMPORTCONTROL settings.
CLIENT	If enabled, the Telnet Comport Control Option negotiation is enabled on specified port when a Telnet connection is initiated.
SERVER	If enabled, the Telnet Comport Control Option negotiation is enabled on the server when a Telnet connection is initiated.
CLIENT TOGGLES DTR	If enabled, the RFC has been negotiated successfully, and the server side sends us a NOTIFY-MODEMSTATE sub packet informing us that DCD has come high(or low), we as the client will raise(or lower DTR) accordingly on our port.
SERVER RAISES DTR	If enabled, and the RFC has been negotiated successfully, then we as the client will send a "SET-CONTROL" sub packet requesting that the server side raise it's DTR signal on the port. This is done once per session.

Overview

The Telnet protocol defines an interactive, character-oriented communications session. It was originally designed to establish a session between a client and a remote login service running on a host. Many new business functions require a person to connect to remote services to retrieve or deposit information. By in large, these remote services are accessed via an asynchronous dial-up connection. This new class of functions include:

- Dial-up connections to the Internet
- Connecting to bulletin boards
- Connecting to internal and external databases
- Sending and receiving faxes.

The general nature of this new class of function requires an interactive, character-oriented communications session via an asynchronous modem. This is typically known as *outbound modem dialing.*

To help defer the cost of installing and maintaining additional phone lines which may be used very little per person, many equipment manufacturers have added the ability to establish a Telnet session directly to the outbound ports on many of the most popular access servers and routers, here after referred to as access servers.

However, the current Telnet protocol definitions are not sufficient to fully support this new use. There are three new areas of functionality which need to be added to the Telnet protocol to successfully support the needs of outbound modem dialing. These are:

- The ability for the client to send com port configuration information to the access server which is connected to the outbound modem. This is needed to ensure the data being transmitted and received by the modem is formatted correctly at the byte level.
- The ability for the access server to inform the client of any modem line or signal changes such as RLSD changes (carrier detect). This information is vital, since many client software packages use this information to determine if a session with the remote service has been established.
- The ability to manage flow control between the client and the access server which does not interfere with the flow control mechanisms used by the session between the client and the remote service.

How Xyplex Implemented this New Functionality

We have implemented the three new areas of functionality, as follows:

- A "limited" client (explained under Client Side Particulars).
- A "server side"(explained under Server Side Particulars and Restrictions. See below and the RFC for more detail).
- Flow control has been implemented from the client (not ours) to server. For example, the server side (Xyplex Access Server) will respond to flowcontrol "suspends" and "resumes" from the client.

Server Side Particulars and Restrictions

We will accept all of the client's request and respond to them(see the RFC for more) except:

- If the client sends us a "SIGNATURE" sub packet with text included, we(as the server side) will not respond to or act on it unless there is no text, then we will follow the spec and send back what our signature is. At this time, it is hardcoded as an uppercase "X".
- If the server side sees a "SET-CONTROL" sub packet from the client for inbound flow control requests, we will just respond with the flow control that we are doing on the port at that time. We have no plans to separate our flow control into inbound and outbound.
- There is no support in this release for the "PURGE-DATA" sub packet from the client. We will ignore any requests in this manner from the client.

Client Side Particulars:

We have implemented a "limited" client side to our software. The following quote from RFC2217 is included for clarity:

"As initially proposed, com port configuration commands are only sent from the client to the access server. There is no current vision that the access server would initiate the use of a com port configuration command, only the notify commands."

Basically, our client will only do the following:

1. Send the Com Port Control option protocol negotiation.

2. Send a hardcoded "SET-MODEMSTATE-MASK" sub packet to the server side with a value of 255. The value of 255 means that we will allow the server side to send any modem state changes that occur on the server side's port via the sub packet route to the client. This is done only once per telnet connection.

3. Send a hardcoded "SET-LINESTATE-MASK" sub packet to the server side with a value of 0. 0 means that we will NOT allow the server side to send any line state changes that occur on the server side's port via the sub packet route to the client. This is done only once per telnet connection.

4. If the server side sends us a NOTIFY-MODEMSTATE sub packet informing us that DCD has come high(or low), we as the client can raise(or lower DTR) accordingly on our port when this feature is enabled.

5. Upon a telnet connection, we as the client can send a "SET-CONTROL" sub packet requesting that the server side raise its DTR signal on the port when this feature is enabled.

DEFINE/SET PORT TELNET CSI ESCAPE Privilege: N, P

Use this command to specify whether or not eight-bit escape sequences, received by the port during a Telnet session, will be passed to the connection partner unaltered (i.e., as eight-bit sequences), or whether these sequences will be translated into their seven-bit equivalents.

You cannot use this command for parallel ports.

Syntax

```
DEFINE/SET PORT port-list TELNET CSI ESCAPE  [DISABLED]
                                             [ENABLED]
```

Where	Means
DISABLED	Eight-bit escape sequences, received by the port during a Telnet session, will be translated into their seven-bit equivalents before they are passed to the connection partner. This is the default setting.
ENABLED	Eight-bit escape sequences, received by the port during a Telnet session, will be passed to the connection partner unaltered.

Example

```
Xyplex>> DEFINE PORT 5  TELNET CSI ESCAPE ENABLED
```

DEFINE PORT TELNET DEDICATED SERVICE Privileged: P

Use this command to specify whether or not there will be a Telnet destination to which the port is permanently assigned, or that there will be a change made to the current permanent service assignment for the port. This setting automatically connects the port to a dedicated service, whenever a user logs on to that port.

You cannot use a SET command to specify a Telnet dedicated service.

Syntax

```
DEFINE PORT port-list TELNET DEDICATED SERVICE[domain-name:telnet-port number]] KICKSTART"string"

                                    [internet-address:telnet-port number]] USERDATA "string"
```

Where	Means
domain-name	The logical name of the Telnet destination to which the port is permanently assigned. If the specified *domain-name* is not a fully qualified domain-name, the specified name will be concatenated with the default Internet domain-name-suffix.
internet-address	The identity or location on the network of the Telnet destination to which the port is permanently assigned.
:*telnet-port number*	The number of the target Internet protocol or physical port address which will be used for sessions between the port and the Telnet destination to which the port is permanently assigned. Note that the colon character (:) is required to separate the telnet-port number from the *domain-name*. If you do not assign a telnet port number, then the default value of 23 will be used.
KICKSTART "*string*"	The port enters a new port state called "kickstart" as soon as the port receives any serial input. Any garbage characters prefacing the kickstart string are flushed. After the first input character match, any subsequent mismatch changes the port state to logout If there is no more input and the kickstart string match hasn't completed, the server waits up to 5 seconds before logging out. When the connection is successful, the port state changes to the "KICKSTART" state and is connected.
USERDATA "*string*"	The data between quotes " " will display on the Show Port screen. If quote marks are used without characters entered between them, the userdata string will be deleted, but the service will be kept. Use the NONE setting to delete both. To modify a userdata string, you must redefine the service as well as change the data string. See DEFINE PORT TELNET DEDICATED SERVICE USERDATA for guidelines.

Example

```
DEFINE PORT 5 TELNET DEDICATED SERVICE FINANCEHOST.XYPLEX.COM KICKSTART “ALERT”

DEFINE PORT 5 TELNET DEDICATED SERVICE 140.179.244.100 USERDATA “\141\142\143\015\012\000”
```

DEFINE PORT TELNET DEDICATED SERVICE KICKSTART Privilege: P

Use this command to enter a data string that provides a connection to a dedicated service when the input from the serial side matches the defined string. The KICKSTART keyword can be defined along with the userdata "string" and vice versa, but not if autobaud is enabled on the port.

Use the SHOW PORT command to display the current Kickstart setting. This setting displays below the dedicated service setting.

Syntax

DEFINE PORT <*port number*> TELNET DEDICATED SERVICE <*ip-address*>/<*domain-name*> KICKSTART <*data-string*>

Where	Means
ip-address / domain name	Enter either the port number or the domain name.
KICKSTART	The port enters a new port state called "kickstart" as soon as the port receives any serial input. Any garbage characters prefacing the kickstart string are flushed. After the first input character match, any subsequent mismatch changes the port state to logout If there is no more input and the kickstart string match hasn't completed, the server waits up to 5 seconds before logging out. When the connection is successful, the port state changes to the "KICKSTART" state and is connected.

data-string Enter the data string (up to 16 characters). The valid ASCII characters are:

- All printable ASCII characters
- Special escaped ASCII characters:
  \b - backspace
  \t - tab
  \N - linefeed
  \f - formfeed
  \v - vertical tab
  \r - carriage return
  \\ - backslash
- All non-printable ASCII characters in the form \000 -\377 octal(hex 00 - FF)

Note: *See the DEFINE PORT TELNET DEDICATED SERVICE USERDATA command for details on how to define non-printable ASCII characters.*

Example:

```
DEFINE PORT 3 TELNET DEDICATED SERVICE 140.179.244.100 KICKSTART “ALERT”
```

DEFINE PORT TELNET DEDICATED SERVICE USERDATA Privilege: P

Use the following commands to add, delete, and modify userdata strings to a Telnet Dedicated Service. The userdata string is passed to the network partner upon connection.

Use the SHOW PORT command to display the current setting. The userdata string displays underneath the Dedicated Service display on the Show Port screen. The screen displays characters just as you entered them, with the following minor exceptions:

- If an octal equivalent of a printable character or a special escape character is entered, then that printable or special escape character will be displayed.
- If an octal \377(hex FF) is entered, then it will be doubled. (Telnet interprets the FF has an IAC.)
- If spaces (spacebar) are imbedded in the string, they will be interpreted as a hex 20 and sent up to the connection partner. Do not enter spaces within the string unless you want to pass them to the connection partner.

Syntax

```
DEFINE PORT port number TELNET DEDICATED [SERVICE] [ip-address/domain name] USERDATA
"userdata_string"

DEFINE PORT port number TELNET DEDICATED[SERVICE][ip-address/domain name]USERDATA ""

DEFINE PORT port number DEDICATED NONE
```

Note: *The keyword "telnet" is required. If it is omitted, the user will be unable to enter the "userdata" string.*

DEFINE PORT TELNET DEDICATED SERVICE USERDATA (continued)

Where	Means
USERDATA	The data that follows this command will display on the screen.
data-string	The data between quotes " " will display on the Show Port screen. If quote marks are used without characters entered between them, the userdata string will be deleted, but the service will be kept. Use the NONE setting to delete both. To modify a userdata string, you must redefine the service as well as change the data string. The following guidelines apply to the characters within a userdata character string. The string, when computed, can store up to 16 characters. The range is as follows: - All printable ascii characters. - Special escaped ascii characters, including: \b - backspace \t - tab \n - linefeed \f - form feed \v - vertical tab \r - carriage return \\ - backslash All non-printable ascii characters in the form of `\000 -\377` octal(hex 00 - FF). The leading backslash (\) is required for the special escaped and octal characters to be interpreted correctly. In fact, if entering an octal, you will receive an error message if you do not use a value in the range of `\000 - \377.` The above covers the entire ascii chart from 0-255.
NONE	Deletes both the service and userdata string.

Examples

The following examples show how userdata strings convert and display.

The user enters `xyplex\r\n`, as the userdata string. The string is displayed as is, and computes down to a total of 8 characters. The `\r` is a carriage return(hex 0D)and the `\n,` a linefeed(hex 0A).

The hex equivalent of the above string `78 79 70 6c 65 78 0d 0a` is sent to the connection partner.

Note: *Keep in mind that all the rules regarding `TELNET NEWLINE` still apply. If a `\r` (carriage return) is part of the entered string, either a null, linefeed, or nothing will be appended to it, depending on the `TELNET NEWLINE` setting.*

Example 1

A user enters the string `\141\142\143\015\012\000`. The string is displayed as `abc\r\n\000`. The string is sent with Telnet as hex `61 62 63 0d 0a 00`.

Note: *Although four keystrokes were entered for `\141`, only one character (a) was stored and sent.*

DEFINE/SET PORT TELNET DEFAULT Privilege: N, P

Use this command to assign or change the telnet-port number (protocol or physical port address) which the port will use for operations where the user does not specify a telnet-port number. This is used to specify the default "source port" number for outgoing (local access) connections being made from this port to a host. Compare this with the TELNET-REMOTE-PORT NUMBER setting, which is used as the "destination port" for incoming connections.

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list  TELNET DEFAULT [telnet-port number]
```

Where	Means
telnet-port number	The number representing a protocol or physical port address which the port will use for operations where the user does not specify a telnet-port number. The default value is 23.

Example

```
DEFINE PORT 5 TELNET DEFAULT 2500
```

DEFINE/SET PORT TELNET DEFAULT TERMINALS Privilege: P

Use this command to specify the default port number to be used when forming a Telnet session.

Syntax

```
DEFINE/SET PORT TELNET DEFAULT [number]
```

DEFINE/SET PORT TELNET ECHO MODE — Privilege: N, P

Use this command to specify how a connection partner will "echo" (return for display at the screen, or print) characters which are typed at the keyboard of a terminal, during a Telnet session.

This command does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list TELNET ECHO MODE   [LOCAL]
                                             [REMOTE]

                                             [DISABLED
                                             [PASSIVE]
                                             [CHARACTER]
                                             [LINE]

                                             [NOECHO]
```

Where	Means
LOCAL	Characters typed at the keyboard will be echoed by the server.
REMOTE	Characters typed at the keyboard will be echoed by the connection partner, if possible (i.e., the server will attempt to negotiate remote echo). This is the default setting for TELNET ECHO MODE.
DISABLED	Disable Telnet echo negotiations.
PASSIVE	Agree with peer on its preferred Echo mode.
CHARACTER	Use character mode.
LINE	Use line mode
NOECHO	Characters typed at keyboard will not be entered.

Example

```
DEFINE PORT 5 TELNET ECHO MODE LOCAL
```

DEFINE/SET PORT TELNET EOR REFLECTION Privilege: P

Use this command to specify whether or not the server will send an End-of-Record (EOR) message back to the host when the server detects an EOR message at the end of the data sent by the host.

For some UNIX hosts, it is necessary for the print filter to add an EOR (End of Record) "handshake" to the end of the data in a print job or there is a risk that the connection will be closed before the print job is completed. Using EOR messages, the port and the print filter will not close the connection until the handshaking is complete, thus guaranteeing that all data is delivered to the port. To use this feature, you must set the PORT TELNET EOR REFLECTION to ENABLED for the port to which the printer is connected, and you must compile the print filter using the -eor option. See the *Printer Configuration Guide* for more information. You must enable or disable EOR handshaking at both the port and the host or connections may not properly be closed when they should be.

Syntax

```
DEFINE/SET PORT port-list TELNET EOR REFLECTION [DISABLED]
                                                [ENABLED]
```

Where	Means
DISABLED	The server will not send an EOR message back to the host, when the server detects an EOR message at the end of the data sent by the host. This is the default.
ENABLED	The server will send an EOR message back to the host, when the server detects an EOR message at the end of the data sent by the host. You must only set this characteristic to ENABLED when EOR messages are being used by both the host and the server.

Example

```
DEFINE PORT 5 TELNET EOR REFLECTION ENABLED
```

DEFINE/SET PORT TELNET ERASE CHARACTER Privilege: S, N, P

Use this command to specify whether or not there will be a character which, when typed by a user in a Telnet session, deletes the character immediately to the left of the cursor.

This command does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list TELNET ERASE CHARACTER   [character]
                                                   [NONE]
```

Where	Means
character	The character which, when typed by a user in a Telnet session, deletes the character immediately to the left of the cursor. It is recommended that you specify an unused CTRL. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, BACKWARD SWITCH, FORWARD SWITCH, or the LOCAL SWITCH settings, line editing commands, or other Telnet command characters).
NONE	There will not be a character which, when typed by a user in a Telnet session, deletes the character immediately to the left of the cursor. This is the default setting.

Example

```
DEFINE PORT 5 TELNET ERASE CHARACTER ^K
```

DEFINE/SET PORT TELNET ERASE LINE Privilege: S, N, P

Use this command to specify whether or not there will be a character which, when typed by a user in a Telnet session, deletes all data in the current line of input, backwards from the cursor position to a prompt or a carriage-return/line-feed

This command does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list  TELNET ERASE LINE [character]
                                             [NONE]
```

Where	Means
character	The character which, when typed by a user in a Telnet session, deletes all data in the current line of input, backwards from the cursor position to a prompt or a carriage-return/line-feed. It is recommended that you specify an unused CTRL character. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, with the character you set for the BACKWARD SWITCH, FORWARD SWITCH, or the LOCAL SWITCH settings, or any other Telnet command characters). If your network supports both LAT and Telnet sessions, you may minimize user confusion caused by switching among different session types if you specify a VMS equivalent to the TELNET ERASE LINE setting (in this case CTRL/U).
NONE	There will not be a character which, when typed by a user in a Telnet session, deletes all data in the current line of input, backwards from the cursor position to a prompt or a carriage-return/line-feed. This is the default setting. You can also use this setting to cancel a previously defined Erase Line character.

Example

```
DEFINE PORT 5 TELNET ERASE LINE ^U
```

DEFINE/SET PORT TELNET INTERRUPT Privilege: S, N, P

Use this command to specify whether or not there will be a character which, when typed by the user in a Telnet session, suspends, interrupts, aborts, or terminates a user process

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list  TELNET INTERRUPT  [character]
                                             [NONE]
```

Where	Means
character	The character which, when typed by a user in a Telnet session, suspends, interrupts, aborts, or terminates a user process. It is recommended that you specify an unused CTRL character. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, with the character you set for the BACKWARD SWITCH, FORWARD SWITCH, or the LOCAL SWITCH setting, or any other Telnet command characters). If your network supports both LAT and Telnet sessions, you may minimize user confusion caused by switching among different session types if you specify a VMS equivalent to the TELNET INTERRUPT setting (in this case CTRL/C).
NONE	There will not be a character which, when typed by the user in a Telnet session, suspends, interrupts, aborts, or terminates a user process. This is the default setting. You can also use this setting to cancel a previously defined interrupt character.

Example

```
DEFINE PORT 5 TELNET INTERRUPT ^C
```

DEFINE/SET PORT TELNET INTERRUPTS AS BREAK Privilege: P

Use this command to define a port to interpret a TELNET interrupt from the network as a TELNET BREAK and send the break out the serial port.

Use the SHOW/LIST PORT TELNET CHARACTERISTICS command to display the current setting. If enabled, it displays in the Enabled Characteristics section.

Notes: *The BREAK TYPE must be set to REMOTE. Use the SHOW PORT command to display the current setting. The Telnet connection cannot be in Transparent mode for the Telnet break to work (transparent mode does not recognize Telnet special characters).*

Syntax

```
DEFINE PORT <port number> TELNET INTERRUPTS AS BREAK  [ENABLED]
                                                      [DISABLED]
```

Where	Means
ENABLED	The port will interpret a Telnet interrupt as a Telnet break and send the break out the serial port.
DISABLED	The port will not interpret a Telnet interrupt as a Telnet break. This is the default.

Example

```
DEFINE PORT 7 TELNET INTERRUPTS AS BREAK ENABLED
```

DEFINE/SET PORT TELNET DEFAULT LOCATION Privilege: P

Use this command to specify whether Telnet will initiate SEND LOCATION option negotiations on specified ports.

Syntax

```
DEFINE PORT [port-list] TELNET DEFAULT LOCATION    [ENABLED]
                                                   [DISABLED]
```

Where	Means
ENABLED	Telnet will use option negotiations to send on the specified port(s).
DISABLED	Telnet will not use option negotiations on the specified port(s). This is the default.

DEFINE/SET PORT TELNET NEWLINE Privilege: S, N, P

Use this command to specify the character(s) that the server should transmit to the connection partner in a Telnet session, when the user presses the RETURN key.

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list  TELNET NEWLINE [NULL]
                                          [LINEFEED]
                                          [NOTHING]
```

Where	Means
NULL	The server should send a carriage-return and a NULL character to the connection partner in a Telnet session, when the user presses the RETURN key. This is the default.
LINEFEED	The server should send a carriage-return and a line-feed character to the connection partner in a Telnet session, when the user presses the RETURN key.
NOTHING	The server should only send a carriage-return character to the connection partner in a Telnet session, when the user presses the RETURN key

Example

```
Xyplex>> DEFINE PORT 5 NEWLINE LINEFEED
```

DEFINE/SET PORT TELNET NEWLINE FILTERING Privilege: S, N, P

Use this command to specify whether or not the server should translate Telnet new-line sequences going from the network to the serial devices, and if it is translating these sequences, in what manner it will perform this translation.

Syntax

```
DEFINE/SET PORT port-list TELNET NEWLINE FILTERING [NONE]
                                                   [LINEFEED]
                                                   [CR]
                                                   [NULL]
                                                   [STANDARD]
```

Where	Means
NONE	The server should not translate Telnet new-line sequences. This is the default setting.
CR	The server should translate Telnet new-line sequences by changing a CR/NULL or CR/LF in the data stream to a CR. This setting is recommended for port 0 (console port).
NULL	The server should translate Telnet new-line sequences by changing a CR or CR/LF in the data stream to a CR/NULL.
LINEFEED	The server should translate Telnet new-line sequences by changing a CR/NULL or CR in the data stream to a CR/LF.
STANDARD	The server should translate Telnet new-line sequences by changing a CR/NULL in the data stream to a CR.

Example

```
DEFINE PORT 5 TELNET NEWLINE FILTERING CR
```

DEFINE/SET PORT TELNET OPTION DISPLAY Privilege: N, P

Use this command to specify whether or not the port should display Telnet option negotiations. This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list TELNET OPTION DISPLAY [DISABLED]
                                                [ENABLED]
```

Where	Means
DISABLED	The port will not display Telnet option negotiations. This is the default setting.
ENABLED	The port will display Telnet option negotiations.

Example

```
DEFINE PORT 5 TELNET OPTION DISPLAY ENABLED
```

DEFINE/SET PORT TELNET PASS8D Privilege: P

Use this command to set the port to function at 8 bits. This allows an 8D (8 bits, even parity) to be passed to the Telnet connection partner as is (not converted). When this feature is enabled, it displays as an Enabled Characteristic on the SHOW/LIST PORT TELNET CHARACTERISITCS screen.

Syntax

```
DEFINE/SET PORT [port-list] TELNET PASS8D [ENABLED]
               [ALL]                      [DISABLED]
```

Where	Means
port-list	Specify which ports will to enable/disable for PASS8d.
ALL	All ports on the will have PASS8d enabled/disabled.
ENABLED	If enabled, an 8D is passed into a serial port doing 8 bits and parity during a Telnet session and will be transmitted to the connection partner unaltered.
DISABLED	If disabled (the default), the 8D will be converted to a 0D as usual.

Example

```
DEFINE PORT 3-8 TELNET PASS8D ENABLED
```

DEFINE/SET PORT TELNET PREFERRED SERVICE Privilege: N, P

Use this command to specify whether or not there will be a Telnet destination to which the port will connect whenever a user makes a connect request without specifying a service or that there will be a change made to the current preferred service assignment for the port.

Note: *When you define a port for preferred service the user will still be able to access the Xyplex prompt when disconnected from the preferred host. When you define a port as Dedicated Service the user will not see the prompt when disconnected.*

Syntax

```
DEFINE/SET PORT port-list TELNET PREFERRED SERVICE   [domain-name[:telnet-port number]]
                                                     [internet-address[:telnet-port number]]
```

Where	Means
domain-name	The logical name of the Telnet destination to which the port will be connected, whenever a user makes a connect request without specifying a domain-name. If the specified domain-name is not a fully qualified domain-name, the specified name will be concatenated with the default Internet domain-name-suffix.
internet-address	The identity or location on the network of the Telnet destination to which the port will be connected, whenever a user makes a connect request without specifying an internet-address.
:telnet-port number	The number of the Internet protocol or physical port address which will be used for sessions between the port and the Telnet destination to which the port will be connected, whenever a user makes a connect request without specifying a Telnet destination. If the Telnet number is not specified, then the Telnet default of 23 will be used.

Examples

```
DEFINE PORT 5 TELNET PREFERRED SERVICE FINANCEHOST.XYPLEX.COM

DEFINE PORT 5 TELNET PREFERRED SERVICE 140.179.244.100
```

DEFINE/SET PORT TELNET QUERY Privilege: S, N, P

Use this command to specify whether or not there will be a character which, when typed by a user in Telnet session, provides a user with a visible indication that the system is still up and running. This command is useful when a user feels that a session has been unexpectedly "silent" for a long time (this could be due to an unusually heavy load on the network or connection partner, or because an operation requires an unanticipated amount of time to complete, etc).

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list  TELNET QUERY   [character]
                                          [NONE]
```

Where	Means
character	The character which, when typed by a user in a Telnet session, displays a visible indication that the system is still up and running. It is recommended that you specify an unused CTRL character. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, with the character you set for the BACKWARD SWITCH, FORWARD SWITCH, or the LOCAL SWITCH settings, line-editing command, or any other Telnet command characters). If your network supports both LAT and Telnet sessions, you may minimize user confusion caused by switching among different session types if you specify a VMS equivalent to the TELNET QUERY setting(in this case CTRL/T).
NONE	There will not be a character which, when typed by a user in a Telnet session, provides a user with a visible indication that the system is still up and running. This is the default setting.

Example

```
DEFINE PORT 5 TELNET QUERY ^T
```

DEFINE/SET PORT TELNET REMOTE Privilege: P

Use this command to assign or change the telnet-port number offered on the network for one or more physical server ports. This allows multiple ports to have the same telnet-port number, so that any of these physical ports are available to service Telnet connection requests, made to a specific telnet-port number. This is used to specify the default destination port number for incoming (remote access) connections being made to this port from a host.

Syntax

DEFINE/SET PORT *port-list* TELNET REMOTE [*telnet-port number*]

Where	Means
telnet-port number	The telnet-port number offered on the network as the address for one or more physical ports. More than one port can have the same remote port number. Assigning the same remote port number to multiple ports allows them to be part of the same logical group (for example, several ports can be part of a bank of dialout ports, each of which have the same address). The default value is [2000 + (100 x *n*)], where *n* is the physical server port number.

Example

EFINE PORT 5-8 TELNET REMOTE 2500

DEFINE/SET PORT TELNET RS491 Privilege: P

Use this command to enable flow control on a port for TELNET RS491.

Syntax

```
DEFINE PORT TELNET RS491 [DISABLED]
                         [ENABLED]
```

Where	Means
Disabled	Disable Telnet RS491 on a port. This is the default.
Enabled	Enable flow control on a port for Telnet RS491.

Example

```
DEFINE PORT TELNET RS491 ENABLED
```

DEFINE/SET PORT TELNET SYNCHRONIZE Privilege: S, N, P

Use this command to specify whether or not there will be a character which, when typed by a user in a Telnet session, allows the user to regain control of a "runaway" process.

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list TELNET SYNCHRONIZE [character]
                                             [NONE]
```

Where	Means
character	The character which, when typed by a user in a Telnet session, allows the user to regain control of a runaway process. It is recommended that you specify an unused CTRL character. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, with the character you set for the BACKWARD SWITCH, FORWARD SWITCH, or the LOCAL SWITCH, or any other Telnet command characters).
NONE	There will not be a character which, when typed by a user in a Telnet session, allows the user to regain control of a runaway process. This is the default setting.

Example

```
DEFINE PORT 5 TELNET SYNCHRONIZE ^K
```

DEFINE/SET PORT TELNET TERMINALTYPE Privilege: N, P

Use this command to specify whether or not the port emulates a particular terminal type during a TELNET or RLOGIN session. The server uses the terminal type you specify during Telnet option negotiations. Refer to the documentation supplied with your host Telnet implementation for a list of valid Telnet terminal types.

Syntax

```
DEFINE/SET PORT port-list  TELNET TERMINALTYPE "terminal-type"
```

Where	Means
terminal-type	The terminal type to be used during a TELNET or RLOGIN session. Valid values are text strings up to 21 characters long. You must enclose the *terminal-type* string in quotation marks (").

Example

```
DEFINE PORT 5 TELNET TERMINALTYPE "VT220"
```

DEFINE/SET PORT TELNET TN3270 DEFAULT PORT Privilege: P

Use this command to assign a default port number for the access server to use when forming a TN3270 session. If you do not specify a default, the access server uses the default port for a Telnet session, which is 23.

Syntax

```
DEFINE/SET PORT [port-list] TELNET TN3270 DEFAULT PORT [port number]
```

Where	Means
port number	The number of the port the access server uses when forming a TN3270 session. Valid values are 1 through 32767. The default value is 23.

Example

```
DEFINE PORT 5 TELNET TN3270 DEFAULT PORT 987
```

DEFINE/SET TERMINAL TELNET TN3270 DEFAULT Privilege: P

Use this command to assign a default port number for the access server to use when forming a TN3270 session using the TN3270 HOST command. If you do not specify a default, the access server uses the default port for a Telnet session.

Syntax

```
DEFINE/SET TERMINAL TELNET TN3270 DEFAULT [port number]
```

Where	Means
ip-port number	The port number used by the access server when forming a TN3270 session.

Example

```
DEFINE PORT TELNET TN3270 DEFAULT 5
```

DEFINE/SET PORT TELNET TN3270 DEVICE Privilege: P

Use this command to indicate whether or not the ports you specify will emulate a particular terminal type during a TN3270 session. If you specify a device name, the access server will automatically assign the USENGLSH TN3270 translation to the ports you specify with this setting. If you want to assign a different translation table to these ports, use the DEFINE/SET PORT TELNET TN3270 TRANSLATIONTABLE command.

Syntax

```
DEFINE/SET PORT [port-list]  TELNET TN3270 DEVICE  [device-name]
                                                   [NONE]
```

Where	Means
device-name	The type of terminal that the ports will emulate during a TN3270 session. You can use the name of a device supplied by Xyplex (ANSI, VT100, VT220-7, or VT220-8), or the name of a device table you have created. See the TN3270 section in the *Advanced Configuration Guide* for more information about how to create device tables.
NONE	Disable the terminal emulation feature. This is the default setting.

Example

```
DEFINE PORT 5 TELNET TN3270 DEVICE ANSI
```

DEFINE/SET PORT TELNET TN3270 EOR Privilege:P

Use this command to enable or disable end of record (EOR) before binary negotiation when establishing a TN3270 session.

Syntax

```
DEFINE/SET PORT [port-list] TELNET TN3270 EOR   [ENABLED]
                                                [DISABLED]
```

Where	Means
ENABLED	End of Record will be used during TN3270 sessions from this port(s).
DISABLED	No End of Record will be used. This is the default.

Example

```
DEFINE PORT 4 TELNET TN3270 EOR ENABLED
```

DEFINE/SET PORT TELNET TN3270 ERRORLOCK Privilege: P

Use this command to enable or disable ErrorLock during a TN3270 session.

Syntax

```
DEFINE/SET PORT [port-list] TELNET TN3270 ERRORLOCK [ENABLED]
                                                    [DISABLED]
```

Where	Means
ENABLED	During a TN3270 session, the terminal will lock when you press an incorrect key sequence until you press the Reset key.
DISABLED	An incorrect key sequence will not cause the terminal to lock.

Example

```
DEFINE PORT 4 TELNET TN3270 ERRORLOCK ENABLED
```

DEFINE/SET PORT TELNET TN3270 PREFIXKEYMAP Privilege: P

Use this command to allow you to define prefix keymaps. Prefix function keys allow you to define hex sequences that get prepended to other function keys' hex values. The maximum size of the prefix function (1 or 2) is 8 bytes. You can combine 3 keys into the prefix and have those 3 keys prefix the "main" key. When the operator then keys the "main" key, (the one with the FF or FE beginning the hex string), the entire prefix string plus the "main" key is sent to the host.

Syntax

```
DEFINE/SET PORT TELNET TN3270 PREFIXKEYMAP [ENABLED]
                                           [DISABLED]
```

Where	Means
ENABLED	The port will allow prefix keymaps.
DISABLED	Keymaps are not allowed. This is the default setting.

DEFINE/SET PORT TELNET TN3270 PRINTER PORT Privilege: P

A server can support two or more local printers for TN3270 screen printing. You can assign printers to specific ports, so that the printing always occurs on those ports.

To enable support for screen printing, assign the ACCESS PRT3270 setting to one or more ports. The TN3270 printer ports must have valid device names.

The SHOW/LIST/MONITOR PORTS TELNET CHARACTERISTICS display shows the TN3270 printer port assignment, or ANY if you have not specified a port.

To set up normal 80-column printing on a server port, use the following commands:

DEFINE PORT *port-list* ACCESS PRT3270
DEFINE PORT *port-list* TELNET TN3270 DEVICE VT100
DEFINE PORT *port-list* AUTOBAUD DISABLED
DEFINE PORT *port-list* SPEED *baud-rate*
DEFINE PORT *port-list* PARITY *parity*
DEFINE PORT *port-list* CHARACTER SIZE *character-size*
LOGOUT PORT *port-list*

See the command pages in this guide for more information about these commands. Refer to the TN3270 section of the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE/SET PORT port-list TELNET TN3270 PRINTERPORT [port number]
                                                    [ANY]
```

Where	Means
port-list	One or more access server ports that you want to assign to a printer port for local TN3270 screen printing.
ANY	Use any available port with ACCESS PRT3270 enabled to print the screen.
port number	Any valid port number with ACCESS PRT3270 enabled and a valid TN3270 device name. When you assign a printer port to a port, the port becomes a dedicated printer port for TN3270 users on the access server.

Example

```
DEFINE PORT 3 TELNET TN3270 PRINTER PORT 4
```

DEFINE PORT TELNET TN3270 SCANNER Privilege: P

Use this command to configure a Telnet TN3270 port as a scanner device. When you enable SCANNER on a port, and console input is detected, the TN3270 will start converting each character from ASCII to EBCDIC and will continue to convert characters until an end of record (Hex0D) is found or an EOB is reached. When the end of record is reached, the entire contents of the buffer will be sent to the Host. Most TN3270 character processing is bypassed which allows this device to convert well over a thousand characters per second.

Note: *TN3270 keymaps are not used with this feature. However, you must still define a device so that TN3270 negotiations work. Normal keyboard lock and unlock still functions with a scanner device enabled, therefore the Host application needs to ensure that when the scanner starts sending characters to the host the keyboard is on in the WCC.*

Syntax

```
DEFINE PORT <port-list> TELNET TN3270 SCANNER [ENABLED]
                                              [DISABLED]
```

Where	Means
ENABLED	Activates the scanner.
DISABLED	Disables the port as a scanner and returns the port to normal TN3270 processing. This is the default.

Example

```
DEFINE PORT 3 TELNET TN3270 SCANNER ENABLED
```

DEFINE PORT TELNET TN3270 SPACE_INSERT Privilege: P

Use this command to enable insert mode on space-filled fields using the TN3270 Insert Mode. See the TN3270 section in the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE PORT TELNET TN3270 SPACE_INSERT [Enabled]
                                       [DISABLED]
```

Where	Means
Enabled	Insert mode will work on space-filled fields.
Disabled	Insert mode will not work on space-filled fields.

Example

```
DEFINE PORT TELNET TN3270 SPACE_INSERT ENABLED
```

DEFINE/SET PORT TELNET TN3270 TRANSLATIONTABLE Privilege: P

Use this command to assign a TN3270 language translation table to the ports you specify. You can also define your own language translation tables. See the TN3270 section of the *Advanced Configuration Guide* for more information about how to create translation tables.

Syntax

```
DEFINE/SET PORT port-list TELNET TN3270 TRANSLATIONTABLE    [trans-name]
                                                            [NONE]
```

Where	Means
trans-name	The name of the TN3270 translation table that the server will use at these ports during Tn3270 sessions. The default is USENGLSH (American English), which the server automatically assigns to ports when you assign them a TN3270 device type.
NONE	Do not assign a TN3270 translation table to these ports. If you have assigned a TN3270 device at these ports, you cannot specify NONE as the translation table. Ports that have TN3270 devices must also have translation tables.

Example

```
DEFINE PORT 5 TELNET TN3270 TRANSLATIONTABLE USENGLSH
```

DEFINE PORT TELNET TN3270 TYPE_AHEAD Privilege: P

Use this command to prevent the buffering of keys in the user console buffer when the keyboard is locked via TN3270. If TypeAhead is enabled, you can also specify the size of the buffer for TN3270 sessions.

This setting does not apply to parallel ports.

Syntax

```
DEFINE PORT TELNET TN3270 TYPE_AHEAD [ENABLED]
                                     [DISABLED]

DEFINE PORT TELNET TN3270 TYPE_AHEAD [buffer-size]
```

Where	Means
ENABLED	Buffering will be prevented.
DISABLED	Buffering of keys will not be prevented.
buffer-size	The size of the typeahead buffer (the number of bytes or characters that can be temporarily stored pending transmission) for sessions at your port, the port(s) specified in the port list, or all ports.

Example

```
DEFINE PORT TELNET TN3270 TYPE_AHEAD ENABLED
```

DEFINE/SET PORT TELNET TN3270 XTDATTRS Privilege: P

Use this command to specify whether or not extended screen attributes will be supported at the ports you specify during a TN3270 session. These attributes include blink, reverse video, underline, and color.

Note: *This feature requires a minimum of 2 MB memory.*

Syntax

```
DEFINE/SET PORT port-list TELNET TN3270 XTDATTRS   [DISABLED]
                                                   [ENABLED]
```

Where	Means
ENABLED	The port will support extended attributes at the ports you specify during a TN3270 session.
DISABLED	Do not enable the extended attributes feature. This is the default setting.

Example

```
DEFINE PORT 5 TELNET TN3270 XTDATTRS ENABLED
```

DEFINE/SET PORT TELNET TRANSMIT Privilege: N, P

Use this command to specify when the server will transmit characters that are typed at a keyboard during a Telnet session. This setting is ignored if TELNET ECHO MODE is set to REMOTE.

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list TELNET TRANSMIT     [BUFFERED] [buffered-time]
                                              [IMMEDIATE]
                                              [IDLETIME] [character-times]
```

Where	Means
BUFFERED	The server will not transmit characters typed at the keyboard until the buffered timer expires. This is the default with a *buffered-time* value of 80 milliseconds. The valid values are 30-1500 milliseconds. Every time the timer expires, any characters that are accumulated in the buffer are sent to connection partner.
buffered-time	The buffered time. 80 milliseconds is the default value. If you omit a buffered time, the default of 80 ms is used.
IMMEDIATE	The server will send each character as soon as possible after it is typed at the keyboard.
IDLETIME	Define or change the maximum amount of time that the server will wait before transmitting the data in the typeahead buffer to the connection partner. You can also specify when the server will transmit user input from a Telnet or RLOGIN session. The server will wait until the port has been idle for the specified period of time, or until the amount of accumulated data exceeds 80% of the typeahead buffer size. This setting is useful when the device connected to the port waits until a control character (such as the RETURN key) is typed at the keyboard, before it transmits data in the typeahead buffer (for example, data that the user has typed, or from a modem). This setting tells the port to send the data at the specified time, even though the control character has not been typed. Use this setting for ports that have their ACCESS setting as REMOTE or DYNAMIC. IDLETIME helps to limit the amount of network traffic when the device connected to the port does not need remote echoing of data.

character-times The maximum amount of time, specified as a number of characters, that the server will wait before transmitting the data in the typeahead buffer to the connection partner. Valid values are between 1 to 255 characters. The default value is 1. If you do not specify a character time, the default is used.

To determine how much time that the server can wait before it will transmit the data in the typeahead buffer to the connection partner, convert *character-times* into seconds, as follows:

Actual delay time = character time* (= times) character size / (= divided by) PORT SPEED.

For example, for a port that has a port-speed of 2400 baud, 8 bits per character, and a TELNET TRANSMIT IDLETIME value of 255, the server will wait 0.85 seconds to transmit data in the typeahead buffer to the connection partner.

Example

```
DEFINE PORT 5 TELNET TRANSMIT IDLETIME 1
```

DEFINE/SET PORT TELNET URGENT BREAK Privilege: P

The Telnet Urgent Break feature determines whether or not a Break sequence is marked "Urgent" when sent to a partner in a Telnet session.

Syntax

```
DEFINE/SET PORT port-list TELNET URGENT BREAK   [ENABLED]
                                                [DISABLED]
```

Where	Means
ENABLED	Break sequences are marked "Urgent" when sent to a partner in a Telnet session.
DISABLED	Break sequences are not marked "Urgent" when sent to a partner in a Telnet session. This is the default

Example

```
DEFINE PORT TELNET URGENT BREAK ENABLED
```

DEFINE PORT TO DEFAULTS — Privilege: P

Use this command to define specified port(s) back to factory defaults.

Note: *Upon issuing this command, you will be prompted to press <RETURN> or any other key to abort the process. This process will be repeated for each specified port in succession. If you press the <RETURN> key, you will be prompted for the next port. If you press any other key, the process for the current port will be terminated, however all previous ports that you specified will still be valid. The port(s) must be logged out for the change to take effect.*

Restrictions

- Not valid for port 0
- The following parameters are not changed(if defined) when defining the port(s) back to defaults:
  - Internet Security
  - IP Filters
  - IPX Filters

Syntax

```
DEFINE PORT [port-list] TO DEFAULTS
```

Example

```
DEFINE PORT 1-20 TO DEFAULTS
```

DEFINE/SET PORT TYPE — Privilege: S, N, P

Use this command to define or change the type of terminal that is connected the port(s) specified in the port-list. The terminal type affects how the attached device produces output, and how the server performs certain device specific functions. For terminals that support emulation of multiple terminal types, this setting should match the actual terminal setting. The setting for the TYPE only affects the operation of the terminal in local command mode.

This setting does not apply to parallel ports.

Syntax

```
DEFINE/SET PORT port-list TYPE   [ANSI]
                                 [HARDCOPY]
                                 [SOFTCOPY]
```

Where	Means
ANSI	The terminal produces output on a video display and supports ANSI escape sequences. Generally, this type of terminal supports the clear screen function and special cursor control functions, but not line drawing (e.g., any VT100, VT200, VT300 or compatible terminal).
HARDCOPY	The terminal is a hardcopy (e.g., a printing or non-video display) terminal, or will emulate the operation of a hardcopy terminal. Generally, this means that the attached device produces output on paper. When you delete characters for this type of device, the deleted characters are echoed between backslash characters (\).
SOFTCOPY	The terminal produces output on a video display but does not support ANSI escape sequences. This type of terminal does echo character deletions when you use the DELETE key, but does not support line drawing, the clear screen function, or special cursor control functions. This is the default setting.

Example

```
DEFINE PORT 5 TYPE HARDCOPY
```

DEFINE/SET PORT TYPEAHEAD SIZE Privilege: P

Use this command to specify the size of the typeahead buffer (the number of bytes or characters that can be temporarily stored pending transmission) for sessions at the port(s) specified in the port-list.

This setting does not apply to parallel ports.

Syntax

`DEFINE/SET PORT` *`port-list`* `TYPEAHEAD SIZE` *`size`*

Where	Means
size	The number of bytes (characters) that can be stored in the typeahead buffer for sessions at the port(s) specified in the port-list. Valid values are between 80 to 16384. The default setting is 128. You should be careful to limit this value, as the typeahead buffer uses resources from the server's pool.

Example

```
DEFINE PORT 5 TYPEAHEAD SIZE 1024
```

DEFINE PORT ULI — Privilege: P

Use this command to enable or disable the UNIX-like user interface at one or more ports. You can also enable this interface so that it is either the primary interface available to a user, or the only interface that is available to the non-privileged or secure user. (Privileged users will continue to have access simultaneously to both the UNIX-like and DECserver-like user interfaces, regardless of this port setting.)

Syntax

```
DEFINE PORT port number ULI    [ENABLED]
                               [ONLY]
                               [PRIMARY]
                               [DISABLED]
```

Where	Means
ENABLED	Enable the UNIX-like interface on the port. When the user logs on to the port, the DLI is still activated. In this mode, users still have access to all ULI and DLI. This is the default.
ONLY	Enable only the UNIX-like interface on the port. In this mode, users do not have access to DLI commands from the ULI.
PRIMARY	When the user logs on to the port, the ULI is activated. In this mode, users still have access to all DLI commands from the ULI.
DISABLED	Disable the UNIX-like interface on the port. In this mode, users do not have access to ULI commands from the DLI.

Example

```
DEFINE PORT 5 ULI DISABLED
```

DEFINE/SET PORT USER KERBEROS PASSWORD Privilege: N, P

Use this command to assign or change a Kerberos password. When you issue this command, the server prompts you for your current password (old password) and the new password. The server then prompts you to verify the new password by retyping it.

The server queries the Kerberos Master when you change a password. If the Master does not respond, you are asked to try again later.

Note: *This feature is not supported in Kerberos 5.*

Syntax

```
DEFINE/SET PORT USER KERBEROS PASSWORD
```

Example

```
Xyplex> DEFINE PORT USER KERBEROS PASSWORD

Old password>

New password>

Verification>
```

DEFINE/SET PORT USERNAME FILTERING Privilege: N

Use this command to specify the type of filtering (if any) used on the defined username. You can specify none or that the server only allow 7-bit printable characters.

Syntax

```
DEFINE/SET PORT USERNAME FILTERING  [NONE]
                                    [SEVEN_BIT]
```

Where	Means
NONE	Specifies that no filtering be used on the defined username. NONE is the default setting.
SEVEN_BIT	Specifies that the server only allow 7-bit printable characters (such as 0x20 to 0x7e) to be used for the username. The server ignores other characters.

Example

```
DEFINE PORT USERNAME FILTERING SEVEN_BIT
```

DEFINE/SET PORT USERNAME PROMPT Privilege: N, P

Use this command to define or change a username string assigned to a port. This is the prompt the user sees at login. When a user logs in to a port that has a username assigned, the port bypasses the Username prompt. (Depending on PASSWORD setting, the port may display a password prompt. If the PASSWORD is set to DISABLED, the port will display the Xyplex> prompt or connect to a dedicated service.) The username also appears in server displays.

If you manage servers using TSM, do not assign a *username* to port 0, or TSM will not work properly.

Syntax

```
DEFINE/SET PORT <port-list> USERNAME PROMPT <"name">
```

Where	Means
"name"	The name to be assigned to the port. The name can be between 1 to 16 characters. You must enclose the name in quotation marks ("). The server will accept the name exactly as it is specified (including spaces, commas, and upper-case or lower-case letters). To cancel a previously-defined username, specify a null string (e.g., " ").
	The default setting is "Enter username."

Example

```
DEFINE PORT 2,4,6 USERNAME PROMPT "Enter your User Name"
```

DEFINE/SET PORT VERIFICATION — Privilege: S, N, P

Use this command to specify whether or not the server will display informational messages at the port(s) listed in the port-list, whenever a user connects, disconnects, or switches a session.

Syntax

```
DEFINE/SET PORT port-list VERIFICATION   [DISABLED]
                                        [ENABLED]
```

Where	Means
DISABLED	The server will not display informational messages, at the port(s) listed in the port-lists, whenever a user connects, disconnects, or switches a session.
ENABLED	The server will display informational messages whenever a user connects, disconnects, or switches a session. This is the default setting.

Example

```
DEFINE PORT ALL VERIFICATION DISABLED
```

DEFINE PORT WELCOME BEFORE AUTHENTICATION Privilege: P

Use this command on specified port(s) to display the Xyplex Welcome banner before the user is prompted for the Radius, Kerberos or SecurID username and password. If enabled, "Welcome Before Authentication" text displays under Enabled Characteristics on the SHOW PORT CHARACTERISTICS display.

Notes: This is a DEFINE only command for this feature. The port(s) must be logged out for this command to take effect. This feature cannot be enabled on Port 0. If you are using APD, you must enable the DEFINE PORT APD AUTHENTICATION INTERACTIVE command to have the Welcome banner print out first..

Syntax

```
DEFINE PORT [port-list] WELCOME BEFORE AUTHENTICATION [ENABLED]
                                                      [DISABLED]
```

Where	Means
ENABLED	The Xyplex Welcome banner will display before any authentication prompt displays for Radius, Kerberos or SecurID.
DISABLED	This is the default.

Example

```
DEFINE PORT 1,4-7 WELCOME BEFORE AUTHENTICATION ENABLED
```

DEFINE PORT XDM HOST Privilege: P

Use this command to specify the domain name or Internet address of an XDM host. Use the DEFINE PORT XDM QUERY command to specify the query type for that host. Use the SHOW/LIST/MONITOR PORTS ALTERNATE CHARACTERISTICS to display the current settings.

Syntax

```
DEFINE PORT port-list XDM HOST  [domain-name]
                                [internet-address]

                                [NONE]
```

Where	Means
port-list	Specify one or more ports that you want to associate with the XDM HOST
domain-name *internet-address*	The domain name or Internet address of the host that will be the XDM manager for the ports you specify.
NONE	Remove the previously defined domain name or Internet address of an XDM host.

Examples

```
DEFINE PORTS 8-16 XDM HOST 117.153.89.3
```

DEFINE/SET PORT XDM QUERY Privilege: P

Use this command to specify the method that the access server uses to search for an XDM manager. Use the DEFINE/SET PORT XDM HOST command to specify the host first. There are three query types: SPECIFIC, BROADCAST, and INDIRECT. SPECIFIC and INDIRECT query types search for the domain name or Internet address you specify. The BROADCAST query type searches for the XDM host using the access server Internet broadcast address specified in the DEFINE/SET SERVER IP BROADCAST ADDRESS command. The INDIRECT query type is only compatible with version X11R5 X Windows or higher.

Use the SHOW PORT ALTERNATE CHARACTERISTICS to display the current setting.

```
DEFINE PORT port-list XDM HOST [ip-address|domain-name]QUERY [BROADCAST]
                                                             [SPECIFIC]
                                                             [INDIRECT]
```

Where	Means
port-list	Specify one or more ports that you want to associate with the Query Type.
SPECIFIC	The ports you specify search for the host at the location in the *domain-name* or *internet-address* variable, which is the XDM manager.
BROADCAST	The ports you specify search the network for an XDM manager using the Internet broadcast address. If you do not enter a query type BROADCAST will be used. This is the default.
INDIRECT	The ports you specify search for the host at the location in the *domain-name* or *internet-address* variable. This host provides a list of XDM managers on the network.

Examples

```
DEFINE PORT 4 XDM HOST DEV.SUN.COM QUERY TYPE SPECIFIC

DEFINE PORTS 5-7 XDM HOST 123.321.32.23 QUERY TYPE INDIRECT
```

DEFINE PORT XON SEND TIMER Privilege: P

Use this command to add a configurable timer that will cause an XON to be transmitted every 'n' seconds, when the port is connected but not XOFF'ed.

Syntax

```
DEFINE PORT port-list XON TIMER [seconds]
```

Where	Means
seconds	Specify how many seconds between XON sends. The valid values are 0 through 2550 seconds. The default is 10 seconds.

Example

```
DEFINE PORT 3 XON TIMER 10
```

DEFINE PORT XREMOTE Privilege: P

Use this command to determine whether or not a port searches for the XDM host as soon a user logs on to the port, rather than returning the Xyplex command interface.

Syntax

```
DEFINE PORT port-list XREMOTE   [DISABLED]
                                [ENABLED]
```

Where	Means
ENABLED	Enable Xremote at the specified ports. The access server then searches for the XDM host you have defined either with a Specific, Indirect, or Broadcast query type. See the DEFINE PORT XDM HOST command for more information on how to do this.
DISABLED	Disable the Xremote feature at the ports you specify. This is the default setting.

Example

```
DEFINE PORT 5 XREMOTE ENABLED
```

DEFINE/SET SERVER - General Information Privilege: P

The DEFINE SERVER and SET SERVER commands specify or modify server characteristics. Generally, server characteristics control communication between the server and the nodes. Changes that are made using the SET SERVER command take effect immediately and are only in effect until the server is re-initialized. Changes made via the DEFINE SERVER command take effect whenever the server is re-initialized. Changes can be made to take effect both immediately and on a permanent basis when the SERVER CHANGE characteristic is set to ENABLED.

Only privileged users can use the DEFINE SERVER or SET SERVER commands.

The basic syntax for the DEFINE SERVER and SET SERVER commands is:

```
DEFINE SERVER [characteristic(s)]
SET SERVER [characteristic(s)]
```

As shown above, you can define or set multiple server settings with a single command. When you specify more than one server setting with one command, separate the characteristics with one or more spaces, a comma, or any combination of commas and spaces. (Note, however, that the maximum length of a command line is 132 characters.)

This section describes the server settings that can be defined. You will find items which are common variables listed throughout this section. Refer to the section on **Common Variables** at the beginning of this guide.

Valid DEFINE/SET SERVER Commands

Command DEFINE/SET SERVER	Define	Set	Reboot server with INIT DELAY command for changes to take affect
ACCOUNTING ENTRIES	X (P)	—	X
ANNOUNCEMENTS	X (P)	X (P)	—
APD	X (P)	—	X
ARAP DEFAULT ZONE	X (P)	—	—
ARAP NODE NAME	X (P)	X (P)	—
ARAP PASSWORD	X (P)	X (P)	—
BROADCAST	X (P)	X (P)	—
CARDCOPY	—	X (P)	—
CARDCOPY ERASE	—	X (P)	—
CHANGE	X (P)	X (P)	—
CIRCUIT TIMER	X (P)	X (P)	—
CONSOLE LOGOUT	X (P)	X (P)	—
CONTROLLED PORTS	X (P)	—	—
CONTROLLED TERMINALS	X (P)	—	—
DAEMON FINGERD	X (P)	—	X
DAEMON LPD	X (P)	—	X
DAEMON ROUTED	X (P)	—	X
DAEMON RWHOD	X (P)	—	X
DAEMON SYSLOGD	X (P)	—	X
DUMP	X (P)	—	—
DUMP PROTOCOL	X (P)	—	—
EVENTLOG	X (P)	X (P)	—
FORMAT CARD	—	X (P)	—
GET CARD	—	X (P)	—
GROUPS	X (P)	X (P)	—
HEARTBEAT	X (P)	X (P)	—
HELP	X (P)	—	X
IDENTIFICATION	X (P)	X (P)	—
IDENTIFICATION SIZE	X (P)	X (P)	—
IMAGE LOAD PROTOCOL	X (P)	—	—
INACTIVITY TIMER	X (P)	X (P)	—
INTERNET IP REASSEMBLY	X (P)	—	—

(P) - Privileged users. — Not applicable

Valid DEFINE/SET SERVER Commands (continued)

Command DEFINE/SET SERVER	Define	Set	Reboot server with INIT DELAY command for changes to take affect
IP ADDRESS	X (P)	X (P)	—
IP ADDRESS AUTODISCOVERY	X (P)	—	X
IP BROADCAST ADDRESS	X (P)	X (P)	—
IP DEFAULT DOMAIN SUFFIX	X (P)	X (P)	—
IP DOMAIN ADDRESS	X (P)	X (P)	—
IP DOMAIN TTL	X (P)	X (P)	—
IP FILTER	X (P)	X (P)	—
IP FILTER DESTINATION	X (P)	X (P)	—
IP FILTER PROTOCOL	X (P)	X (P)	—
IP FILTER SOURCE	X (P)	X (P)	—
IP FILTER SYN	X (P)	X (P)	—
IP FILTERING	X (P)	X (P)	X
IP GATEWAY ADDRESS	X (P)	X (P)	—
IP GATEWAY TIMEOUT	X(P)	X (P)	—
IP HOST	X (P)	—	—
IP LOAD FILE	X (P)	X (P)	—
IP LOCAL BASE	X (P)	X (P)	—
IP NAME	X (P)	X (P)	—
IP ROTARY	X (P)	X (P)	—
IP ROUTE	X (P)	X (P)	—
IP ROUTING TABLE SIZE	X (P)	—	X
IP SECURITY	X (P)	—	X
IP SNMP AUTHENTICATION TRAPS	X (P)	X (P)	—
IP SNMP CLIENT	X (P)	X (P)	—
IP SNMP COMMUNITY	X (P)	X (P)	—
IP SNMP SYSTEM CONTACT	X (P)	X (P)	—
IP SNMP SYSTEM LOCATION	X (P)	X (P)	—
IP SUBNET MASK	X (P)	X (P)	—
IP SUBNET MASK AUTOCONFIGURE	X (P)	X (P)	—
IP TCP CONNECT TIMER	X (P)	X (P)	—
IP TCP RESEQUENCING	X (P)	—	—

(P) - Privileged users. — Not applicable

Valid DEFINE/SET SERVER Commands (continued)

Command DEFINE/SET SERVER	Define	Set	Reboot server with INIT DELAY command for changes to take affect
IP TCP RETRANSMIT	X (P)	X (P)	—
IP TRANSLATIONTABLE TTL	X (P)	X (P)	—
IP TTL	X (P)	X (P)	—
IPX FILTER DESTINATION	X (P)	X (P)	—
IPX FILTER DESTINATION NODE	X (P)	X (P)	—
IPX FILTER DESTINATION SOURCE	X (P)	X (P)	—
IPX FILTER NETWORK	X (P)	X (P)	—
IPX FILTER PACKET	X (P)	X (P)	—
IPX FILTER SOURCE NETWORK	X (P)	X (P)	—
IPX FILTER SOURCE NODE	X (P)	X (P)	—
IPX FILTERING	X (P)	—	X
IPX INTERNAL NETWORK	X (P)	—	—
IPX NETWORK	X (P)	—	—
IPX PROTOCOL	X (P)	—	X
IPX RIP BROADCAST	X (P)	X (P)	—
IPX RIP BROADCAST DISCARD TIMEOUT	X (P)	X (P)	—
IPX RIP BROADCAST TIMER	X (P)	X (P)	—
IPX RIP EXPORT	X (P)	X (P)	—
IPX RIP MAXIMUM TABLE SIZE	X (P)	—	X
IPX SAP BROADCAST	X (P)	X (P)	—
IPX SAP BROADCAST TIMER	X (P)	X (P)	—
IPX SAP BROADCAT DISCARD TIMEOUT	X (P)	X (P)	—
IPX SAP EXPORT NETWORK	X (P)	X (P)	—
IPX SAP EXPORT TYPE	X (P)	X (P)	—
IPX SAP IMPORT NETWORK	X (P)	X (P)	—
IPX SAP IMPORT TYPE	X (P)	X (P)	—
IPX SAP MAXIMUM TABLE SIZE	X (P)	—	X
IPX TIP IMPORT NETWORK	X (P)	—	—
KEEPALIVE TIMER	X (P)	X (P)	—

(P) - Privileged users. — Not applicable

Valid DEFINE/SET SERVER Commands (continued)

Command DEFINE/SET SERVER	Define	Set	Reboot server with INIT DELAY command for changes to take affect
KERBEROS	X (P)	—	X
KERBEROS ERROR MESSAGE	X (P)	X (P)	—
KERBEROS FIVE	X (P)	—	X
KERBEROS MASTER	X (P)	X(P)	—
KERBEROS PASSWORD PORT	X (P)	X (P)	—
KERBEROS PASSWORD SERVICE	X (P)	X (P)	—
KERBEROS PORT	X (P)	X (P)	—
KERBEROS PRIMARY SERVER	X (P)	X (P)	—
KERBEROS QUERY LIMIT	X (P)	X (P)	—
KERBEROS REALM	X (P)	X (P)	—
KERBEROS SECONDARY SERVER	X (P)	X (P)	—
KERBEROS SECURITY	X (P)	X (P)	—
LAT IMMEDIATE ACK	X (P)	X (P)	—
LAT SOLICITS	X (P)	X (P)	—
LOAD IP ADDRESS	X (P)	—	—
LOAD IP DELIMITER	X (P)	X (P)	—
LOAD IP DELIMITER	X (P)	X (P)	—
LOAD IP GATEWAY	X (P)	—	—
LOAD IP LOAD FILE	X (P)	—	—
LOAD IP LOAD HOST	X (P)	—	—
LOAD PROTOCOL	X (P)	—	—
LOAD SOFTWARE	X (P)	—	—
LOAD STATUS MESSAGE	X (P)	—	—
LOADDUMP	X (P)	—	—
LOADDUMP DEFAULT	X (P)	—	—
LOCK	X (P)	X (P)	—
LOGIN PASSWORD	X (P)	X (P)	—
LOGIN PROMPT	X (P)	X (P)	—
LPD QUEUE	X (P)	X (P)	—
LPD QUEUE BYPASS	X (P)	X (P)	—

(P) - Privileged users. — Not applicable.

Valid DEFINE/SET SERVER Commands (continued)

Command DEFINE/SET SERVER	Define	Set	Reboot server with INIT DELAY command for changes to take affect
MAINTENANCE PASSWORD	X (P)	X (P)	—
MENU	X (P)	—	X
MENU CONTINUE PROMPT	X (P)	X (P)	—
MENU PROMPT	X (P)	X (P)	—
MULTICAST TIMER	X (P)	X (P)	—
MULTISESSIONS	X (P)	—	X
NAME	X (P)	X (P)	—
NESTED MENU NAME	X (P)	—	—
NESTED MENU SIZE	X (P)	—	X
NODE LIMIT	X (P)	X (P)	—
NOPRIVILEGED	—	X (P)	—
NUMBER	X (P)	X (P)	—
OVERRIDE INTERNAL ADDRESS	X (P)	—	—
PACKET COUNT	X (P)	—	X
PAP CHAP REMOTE PASSWORD	X (P)	—	—
PAP REMOTE PASSWORD	X (P)	X (P)	—
PARAMETER SERVER	X (P)	X (P)	—
PARAMETER SERVER CHECK	X (P)	X (P)	—
PARAMETER SERVER LIMIT	X (P)	X (P)	—
PARAMETER SERVER PATH	X (P)	X (P)	—
PARAMETER SERVER RETRANSMIT	X (P)	X (P)	—
PARAMETER VERSION	—	X (P)	—
PASSWORD LIMIT	X (P)	X (P)	—
PRIVILEGED	—	X (P)	—
PRIVILEGED PASSWORD	X (P)	X (P)	—
PROTOCOL ARAP	X (P)	—	X
PROTOCOL IPX	X (P)	—	X
PROTOCOL LAT	X (P)	—	X
PROTOCOL MX800	X (P)	—	—
PROTOCOL PPP	X (P)	—	X
PROTOCOL SNMP	X (P)	—	X

(P) - Privileged users. — Not applicable

Valid DEFINE/SET SERVER Commands (continued)

Command DEFINE/SET SERVER	Define	Set	Reboot server with INIT DELAY command for changes to take affect
PROTOCOL TELNET	X (P)	—	X
PROTOCOL TN3270	X (P)	—	X
PROTOCOL XPRINTER	X (P)	—	X
PROTOCOL XREMOTE	X (P)	—	X
PURGE GROUP	X (P)	X (P)	—
PURGE NODE	X (P)	X (P)	—
QUEUE LIMIT	X (P)	X (P)	—
RADIUS	X (P)	—	X
RADIUS ACCOUNTING	X (P)	X (P)	—
RADIUS CHAP CHALLENGE SIZE	X (P)	X (P)	—
RADIUS LOGGING	X (P)	X (P)	—
RADIUS PORT	X (P)	X (P)	—
RADIUS PRIMARY SECRET	X (P)	X (P)	—
RADIUS PRIMARY SERVER	X (P)	X (P)	—
RADIUS SECONDARY SECRET	X (P)	X (P)	—
RADIUS SECONDARY SERVER	X (P)	X (P)	—
RADIUS SERVER RETRY	X (P)	X (P)	—
RADIUS TIMEOUT	X (P)	X (P)	—
RELIABLE ACCOUNTING	X (P)	X (P)	—
REPORT ERRORS	X (P)	X (P)	—
RETRANSMIT LIMIT	X (P)	X (P)	—
RIP STATE	X (P)	—	X
RLOGIN	X (P)	X (P)	X
ROTARY ROUNDROBIN	X (P)	—	X
SCRIPT SERVER	X (P)	X (P)	—
SECURID	X (P)	—	X
SECURID ACM_PORT	X (P)	X (P)	—
SECURID ACMBASETIMEOUT	X (P)	—	—
SECURID ACMMAXRETRIES	X (P)	X (P)	—
SECURID ENCRYPTION MODE	X (P)	X (P)	—
SECURID QUERY LIMIT	X (P)	X (P)	—
SECURID SERVERn	X (P)	X (P)	—

(P) - Privileged users. — Not applicable

Valid DEFINE/SET SERVER Commands (continued)

Command DEFINE/SET SERVER	Define	Set	Reboot server with INIT DELAY command for changes to take affect
SERVER COPY	—	X (P)	—
SERVER DATE	—	X (P)	—
SERVER TIME	—	X (P)	—
SERVICE	X (P)	X (P)	—
SERVICES GROUPS	X (P)	X (P)	—
SESSION	—	X(P)	—
SESSION LIMIT	X (P)	—	—
SOFTWARE	X (P)	X (P)	—
TCP ACK DELAY	X (P)	X (P)	—
TEXTPOOL SIZE	X (P)	X(P)	X
TIME SERVER	X (P)	X (P)	—
TIMEZONE	X (P)	X (P)	—
TN3270 DEVICE	X (P)	—	—
TN3270 DEVICE KEYMAP NUM_OVERRIDE	X (P)	—	—
TN3270 DEVICE NAME	X (P)	—	—
TN3270 DEVICE SCREENMAP COLOR	X (P)	—	—
TN3270 TRANSLATION TABLE	X (P)	—	—
ULI	X (P)	—	X
USE DEFAULT PARAMETERS	X (P)	—	X
USERDATA DELAY	X (P)	—	—
VERBOSE ACCOUNTING	X (P)	X (P)	—
VERBOSE PRIORITY	X (P)	X (P)	—
WELCOME	X (P)	X (P)	—
XPRINTER	X (P)	X (P)	—
XPRINTER DATA TIMEOUT	X (P)	—	—
XREMOTE FONT SERVER	X (P)	X (P)	—

(P) - Privileged users. — Not applicable

DEFINE SERVER ACCOUNTING ENTRIES Privilege: P

Use this command to change the maximum number of accounting entries that the server will record in the accounting log. To enable the accounting feature, change the number of accounting entries from 0 to any number greater than or equal to 1, then reboot the server using the INIT DELAY command so the change can take effect.

When the accounting feature is enabled, the server creates an accounting log. Each log entry contains information about successful and attempted connections made to or from the unit, as well as information about sessions that are disconnected.

You can view the contents of the accounting log by viewing the SHOW/MONITOR SERVER ACCOUNTING display. See the Accounting section in the *Advanced Configuration Guide* for information about the accounting feature.

This feature requires a minimum of 1 megabyte of free memory.

Syntax

```
DEFINE SERVER ACCOUNTING ENTRIES number
```

Where	Means
number	The maximum number of accounting entries that the server will record in the accounting log. Valid values are between 0 and 1000. The default is 0. Changing the number from 0 to any other number enables the accounting feature. Changing the number to 0 disables the accounting feature.

Example

```
DEFINE SERVER ACCOUNTING ENTRIES 100
```

DEFINE/SET SERVER ANNOUNCEMENTS PRIVILEGE: P

Announcements are multicast messages, which are sent by the server via the Ethernet network to other servers. These messages indicate which LAT services are available at the server. Announcements are only multicast when there are local services defined at the server.

Use this command to enable or disable these multicast messages.

Syntax

```
DEFINE/SET SERVER ANNOUNCEMENTS  [DISABLED]
                                 [ENABLED]
```

Where	Means
DISABLED	The server will not multicast announcements about available services.
ENABLED	The server will multicast announcements about available services. This is the default setting.

Example

```
DEFINE SERVER ANNOUNCEMENTS ENABLED
```

DEFINE SERVER APD ENABLED/DISABLED Privilege: P

Access server ports can be configured to accept connections made via different protocols using the Automatic Protocol Detection (APD) feature. Using APD, ports will automatically determine the protocol being used to make a connection and adjust port settings appropriately. If you do not enable APD, ports can be dedicated for use by a single access serving protocol. An individual port can be configured to accept any connections made via ARAP, PPP, SLIP (which includes CSLIP), and interactive protocols, as well as all or none of these.

After you enable APD on the server, you must reboot the server using the INIT DELAY command and then enable APD-related settings for individual ports. If you do not specify APD-related settings for the ports which use access serving protocols, the ports will default to permitting only interactive connections, unless configured with another protocol.

Several commands are available which control the protocols that will be accepted for APD ports, and other aspects of APD operation. Use this command to configure the server so that ports can accept different types of connections (i.e., using more than one protocol).

See Using the TCP/IP Features in the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE SERVER APD    [ENABLED]
                     [DISABLED]
                     [NONE]
```

Where	Means
ENABLED	Ports on this server can be configured to accept connections made via any combination of ARAP, PPP, SLIP (which includes CSLIP), and interactive protocols, as well as all of these.
DISABLED	Ports on this server cannot be configured to accept connections made via a choice of different protocols. Ports will be limited to one type of connection (for whatever protocol is configured at a given port). This is the default.
NONE	This is the same as DISABLED.

Example

```
DEFINE SERVER APD ENABLED
```

DEFINE/SET SERVER APD MESSAGE Privilege: P

Use this command to change the default APD message string. Use the SHOW UNIT command to display the current APD message string.

Syntax

```
DEFINE SERVER APD MESSAGE <"message-string">
```

Where	Means
"message-string"	The message string can contain up to 80 characters. Make sure to enclose the message in quotes ("). When APD is enabled on the unit, the default message string is: "AutoProtocol Detect - Begin protocol or enter 4 returns for interactive mode."

Example

```
DEFINE SERVER APD MESSAGE "Launch PPP Protocol or hit <enter> 4 times for
interactive mode."
```

DEFINE SERVER ARAP DEFAULT ZONE Privilege: P

All AppleTalk devices are found in an AppleTalk zone, which can be an EtherTalk zone, a TokenTalk zone, a LocalTalk zone, etc. There is always a default choice for the zone which the device will join. Xyplex communication servers join an EtherTalk zone.

The DEFINE/SET SERVER ARAP DEFAULT ZONE command allows the server manager to specify the default EtherTalk zone that the server joins after it is initialized. If there is no zone of that name available on the network segment the server will join the default zone for the segment.

Syntax

```
DEFINE SERVER ARAP DEFAULT ZONE     ["zone-name"]
                                    [NONE]
```

Where	Means
"zone-name"	Specifies the name of the AppleTalk zone that the server will attempt to join when it is initialized. The zone name is a quoted, case-sensitive text string that can be up to 32 characters long and cannot contain the double-quote (") character.
NONE	Specifies that the server will not be assigned to a specific AppleTalk zone. This is the default.

Example

```
DEFINE SERVER ARAP DEFAULT ZONE "REMOTEZONE"
```

DEFINE/SET SERVER ARAP PASSWORD Privilege: P

The server manager can configure a server so that when Remote Access users try to connect, the users must type a login password. There is only one Remote Access login password per server.

Use this command to specify the password that Remote Access users must type when they log on. If you type the password on the DEFINE/SET SERVER ARAP PASSWORD command line, enclose the password in quotation mark characters ("). If you do not type the password on the DEFINE/SET SERVER ARAP PASSWORD command line, the server will prompt you for a password. In this case, do not enclose the password in quotation mark characters. Also, in this case, the server will not echo the password.

Syntax

```
DEFINE/SET SERVER ARAP PASSWORD ["password"]
```

Where	Means
"password"	The new password that Remote Access users must type when they log on to a server port. The password can be up to 8 characters long and cannot contain the double-quote (") character. The password is case-sensitive. The default ARAP password is "access".

Example

```
DEFINE SERVER ARAP PASSWORD "REMOTE"
```

or

```
DEFINE SERVER ARAP PASSWORD

Password > REMOTE
```

DEFINE/SET SERVER ARAP NODE NAME Privilege: P

Use this command to specify the AppleTalk node name that the remote user sees.

When a remotely connected AppleTalk user connects to the network via a Remote Access server, the name of the Remote Access server is displayed in the Remote Access Status display.

The default ARAP node name setting is NONE. If you do not specify a node name, the unit will use the server-name specified by the DEFINE/SET SERVER NAME command By default, the server name is a seven-character name in the form X*nnnnnn*, where *nnnnnn* represents the last 6 digits of the server Ethernet address. For servers that operate with a parameter server that is a VAX/VMS node, the default name is the DECnet node name that has been assigned by the system manager of that node.

Syntax

```
DEFINE/SET SERVER ARAP NODE NAME    ["node name"]
                                    [NONE]
```

Where	Means
"*node name*"	The server's AppleTalk node name. Enclose the node name in quotes ("). It is case-sensitive and can be up to 32 characters. The node name cannot contain the double-quote (") character.
NONE	That the server will not have an AppleTalk node name assigned to it. In this case, the server will revert to using the server-name. This is the default.

Example

```
DEFINE SERVER ARAP NODE NAME "REMOTEMACS"
```

DEFINE/SET SERVER BROADCAST Privilege: P

Use this command to specify whether or not the Broadcast command is available to users at this server. The BROADCAST command allows users at one port to send a message to users at other ports on the server.

Syntax

```
DEFINE/SET SERVER BROADCAST    [DISABLED]
                               [ENABLED]
```

Where	Means
DISABLED	Specifies that the Broadcast command is not available to any users at this server.
ENABLED	Specifies that the Broadcast command is available to users at this server. This is the default setting.

Example

```
DEFINE SERVER BROADCAST ENABLED
```

SET SERVER CARDCOPY Privilege: P

Use this command on units that have flash cards. You can copy the entire contents of one card to another with this command.

Syntax

```
SET SERVER CARDCOPY
```

SET SERVER CARDCOPY ERASE

Use this command on units that have flash cards. You candelete the entire contents of a flash card.

CAUTION

DO NOT USE THIS COMMAND UNLESS YOU ARE ABSOLUTLEY SURE THAT YOU WANT ALL CONTENTS DELETED.

Syntax

```
SET SERVER CARDCOPY ERASE
```

DEFINE/SET SERVER CHANGE Privilege: P

Normally, a DEFINE command affects only the permanent database, and a SET command affects only the operational database.

Use this command to specify whether or not the server will update both the permanent and operational database when a DEFINE command is issued. This has the effect of allowing you to perform both a DEFINE and SET operation with only a DEFINE command, and is particularly useful when first setting up a server or when you need to issue a large number of commands.

SNMP SET commands are not affected by this setting.

Syntax

```
DEFINE/SET SERVER CHANGE    [DISABLED]
                            [ENABLED]
```

Where	Means
DISABLED	Specifies that the server will not update both the permanent and operational database when a DEFINE command is issued. This is the default.
ENABLED	Specifies that the server will update both the permanent and operational database when a DEFINE command is issued.

Example

```
DEFINE SERVER CHANGE ENABLED
```

SET SERVER CHASSIS

Use this command to change the access server settings in the operational database. This command is used only on the Network 9000 720 Access Server. Refer to the Network 9000 documentation for more information.

DEFINE/SET SERVER CIRCUIT TIMER Privilege: P

Use this command to specify how often the server will communicate with service nodes when LAT sessions are active. During the specified time period, the server collects all data from active sessions, multiplexes the data, and creates Ethernet packets. At the end of the interval, the server transmits all of these packets to the appropriate service nodes for processing. Thus, the value set for this option affects the response time for the user, as well as network performance, and performance at the service nodes.

By changing the circuit timer value, you can manage the relationship (or trade-off) between user response time and efficient use of network and service node resources. For example, setting a short time interval means that users receive fast response time, but there is more traffic on the network and service nodes must respond more frequently. A longer time interval means that users receive a slower response time, but there is less network traffic and server nodes must respond less frequently. Thus, you may decide to specify a longer time interval when network or service node performance suffers from heavy use, while lightly loaded network and service node resources can support faster user response times.

Syntax

```
DEFINE/SET SERVER CIRCUIT TIMER timer-value
```

Where	Means
timer-value	The length of the circuit timer interval, in milliseconds. The value specified must be a number between 30 to 200 milliseconds. The default value is 80.

Example

```
DEFINE SERVER CIRCUIT TIMER 100
```

DEFINE/SET SERVER CONSOLE LOGOUT Privilege: P

Use this command to specify whether or not the server will immediately disconnect a console port session when the user logs out from the console port (port 0). This applies to sessions established via REMOTE CONSOLE and TELNET CONSOLE and CHASSIS CONSOLE (Network 9000).

The access server does not immediately disconnect a console port session when this command is enabled, if the user established the session through the REMOTE CONSOLE command. The access server does disconnect the session after about 10 seconds. The access server does immediately disconnect console port sessions established through TELNET CONSOLE, TELNET CONNECT, or CHASSIS CONSOLE if the CONSOLE LOGOUT feature is enabled.

Syntax

```
DEFINE/SET SERVER CONSOLE LOGOUT    [DISABLED]
                                    [ENABLED]
```

Where	Means
DISABLED	The server will disconnect the session 10 seconds after the user logs out. If the user hits the <Return> key again before 10 seconds have passed, they will be prompted for re-entry to port. The server will not immediately disconnect a console port session when the user logs out from the console port.
ENABLED	The server will immediately disconnect a console port session when the user logs out from the console port. This is the default.

Example

```
DEFINE SERVER CONSOLE LOGOUT ENABLED
```

DEFINE SERVER CONTROLLED PORTS Privilege: P

Use this command to enable or disable support for controlled ports. You must first enable controlled ports and then reboot the server before entering further controlled port definitions. Disabling controlled ports can save memory space.

The SET command is not available for this feature.

Syntax

```
DEFINE/SET SERVER CONTROLLED PORTS  [DISABLED] [init-string}
                                    [ENABLED]
```

Where	Means
DISABLED	Support for controlled ports and sessions is turned off. This is the default.
ENABLED	Support for controlled ports and sessions is turned on. You must reboot the server AFTER enabling, and then you can specify an initialization string.
init-string	If enabled, you can enter an initialization string to specify an action for the port take. The string must be in hexadecimal and enclosed by quotes ("").

Example

"61 74 73 30 2B 31" for the initialization string ats0=1 (or higher). This string would enable auto-answer on the first ring on an attached modem. Save the configuration on the modem. For additional information refer to the documentation that accompanied your modem.

Example

```
DEFINE SERVER CONTROLLED PORTS ENABLED

DEFINE SERVER CONTROLLED PORTS "61 74 73 20 2B 31"
```

DEFINE SERVER CONTROLLED TERMINALS Privilege: P

Use this command to enable or disable support for controlled terminals. You must first enable controlled terminals and then reboot the server before entering further controlled terminal definitions. Disabling controlled terminals can save memory space.

The SET command is not available with this feature.

Syntax

```
DEFINE SERVER CONTROLLED TERMINALS        [DISABLED]
                                          [ENABLED]
```

Where	Means
DISABLED	Support for controlled terminals and sessions is turned off. This is the default.
ENABLED	Support for controlled terminals and sessions is turned on.

Example

```
DEFINE SERVER CONTROLLED TERMINALS ENABLED
```

DEFINE SERVER DAEMON FINGERD Privilege: P

Use this command to enable or disable the FINGERD daemon on the server. The FINGERD daemon provides a method for exchanging information between hosts about users who are logged on to a server, using a Finger User Information Protocol (RFC 1288). FINGERD is supported by implementing software at the server, which responds to requests for information about a user made at a UNIX host.

You must reboot the server using the INIT DELAY command for the change to take effect.

See the Daemons section in the *Advanced Configuration Guide* for more information. The Daemons section also shows the type of output that is supplied by the FINGERD daemon.

Syntax

```
DEFINE SERVER DAEMON FINGERD  [DISABLED]
                              [ENABLED]
```

Where	Means
ENABLED	Enable the FINGERD daemon on the server.
DISABLED	Disable the FINGERD daemon on the server. This is the default setting.

Example

```
DEFINE SERVER DAEMON FINGERD ENABLED
```

DEFINE SERVER DAEMON LPD Privilege: P

The LPD daemon provides a method for sending print jobs between UNIX systems and managing jobs that are in a print queue, using a protocol that is defined in RFC 1179. LPD is supported by implementing software at the server, which responds to print requests made at a UNIX host using the Berkeley and AT&T System V UNIX lpr, lpc, lprm, and lpq, commands and the lpstat, enable, and disable commands. The lpc, lpq, and lprmc commands are also available on the Xyplex access server.

See the Daemons section in the *Advanced Configuration Guide* for more information. See the *Using the ULI Guide* for a description of the lpc, lpq, and lprm commands that are available. The UNIX-like Interface must be enabled in order to use the lpc, lpq, and lprm commands at the server.

You must reboot the server using the INIT DELAY command for the change to take effect.

Syntax

```
DEFINE SERVER DAEMON LPD   [DISABLED]
                           [ENABLED]
```

Where	Means
ENABLED	Enable the LPD daemon on the server.
DISABLED	Disable the LPD daemon on the server. This is the default.

Example

```
DEFINE SERVER DAEMON LPD ENABLED
```

DEFINE SERVER DAEMON ROUTED Privilege: P

The ROUTED daemon provides a method for exchanging routing information among gateways or hosts, using the Routing Information Protocol that is defined in RFC 1058. The access server uses this protocol to learn about Internet routes from other hosts or gateways (in this case, the server behaves as though it was a UNIX host). In the Xyplex routed implementation, the server listens for routing messages and updates its internal routing tables, without transmitting any routing information to other gateways or hosts (i.e., the server is a "silent" or "passive" router).

Other methods also used include: Xyplex servers only update their internal routing tables by listening to and storing re-direct messages, or by having routes added by a privileged user via the DEFINE/SET SERVER IP ROUTE command. Internet routes that are learned via RIP or ICMP re-direct messages are lost when the server is re-initialized. Internet routes learned via RIP expire after 5 minutes, unless the server receives another RIP message with the route. All Internet routes that the server knows can be viewed using the SHOW/LIST/ MONITOR IP ROUTES command

See the Daemons section in the *Basic Configuration Guide* for more information. Use the SHOW/MONITOR IP ROUTES command to display the current setting.

You must reinitialize the server using the INIT DELAY command for the change to take effect.

Syntax

```
DEFINE SERVER DAEMON ROUTED   [DISABLED]
                              [ENABLED]
```

Where	Means
ENABLED	Enable the ROUTED daemon on the server.
DISABLED	Disable the ROUTED daemon on the server. This is the default.

Example

```
DEFINE SERVER DAEMON ROUTED ENABLED
```

DEFINE SERVER DAEMON RWHOD Privilege: P

The RWHOD daemon provides a method for collecting information about domain names on the network by listening to "rwho" messages and adding currently unknown domain names to the domai-name table.

Other methods used to collect information include: Xyplex servers only update their domain name tables when the server itself requested a domain name from a Domain Name Server, or by having domain names added by a privileged user via the DEFINE/SET DOMAIN command. Learned domain names are lost when the server is re-initialized. When a server receives an "rwho" message that contains a domain-name that the server has already learned, the time-to-live (TTL) for that domain-name is set to 1 day. All domain names that the server knows can be viewed using the SHOW/LIST/ MONITOR DOMAIN command.

When the server receives an rwho message, if the domain name already exists in the domain-name table, and its source is either the primary or secondary name server, then the entry is overwritten with "Who" as the source and a time-to-live of 1440. If the domain-name exists in the table, and its source is "local," the entry is not overwritten.

See the Daemons section in the *Basic Configuration* for more information. Use the SHOW/LIST/MONITOR DOMAIN command to display the current settings.

You must reboot the server using the INIT DELAY command for the change to take effect.

Syntax

```
DEFINE SERVER DAEMON RWHOD   [DISABLED]
                             [ENABLED]
```

Where	Means
ENABLED	Enable the rwhod daemon on the server.
DISABLED	Disable the rwhod daemon on the server. The daemon is disabled as the factory default.

Example

```
DEFINE SERVER DAEMON RWHOD ENABLED
```

DEFINE SERVER DAEMON SYSLOGD Privilege: P

The syslogd daemon provides a central facility to log messages about events which occur on the server(s). These messages can be logged at the server and/or in a file at a UNIX host. This daemon is part of the Enhanced Event Accounting feature.

This command enables or disables the `syslogd` daemon on the access server and specifies up to two remote hosts which will receive the accounting entries. The remote host(s) must also be running a UNIX implementation of syslogd.

Enabling the `syslogd` daemon provides remote logging of normal or verbose accounting entries. As the access server places each entry into the local account log, it sends a message to the host you specify in the command line (Host1 or Host2). The syslogd intercepts the message and routes it to one or more destinations, depending on the settings in the `/etc/syslog.conf` file on the host. The entries contain the same information in the remote log file as in the access server log file.

See the Daemons section in the *Advanced Configuration Guide* for more information on setting up syslogd. Refer to the Accounting section in the *Basic Configuration Guide* for more information about setting up and using the accounting feature and a description of syslogd output at a UNIX host. Refer to the description of the SHOW/MONITOR SERVER ACCOUNTING command for a description of event log accounting output at a server.

You must reboot the server using the INIT DELAY command for the change to take effect.

Limitations

Please note the following limitations when specifying two syslogd hosts:

- Define Host 1 first.
- Define a unique IP address for each Syslogd host.
- Syslog messages for both hosts must be logged at the same Log Facility
- To delete a Syslogd host, you must first disable Host 2

To display Syslogd host, use the following command:

```
SHOW UNIT
```

Both Syslogd hosts display if they have been previously defined.

DEFINE SERVER DAEMON SYSLOGD (continued)

Note: *If you are upgrading from an earlier revision and already have a Syslogd host defined, then the SHOW UNIT display will now show that host as "Host1" as opposed to "Host."*

Syntax

For Host 1, use:

```
DEFINE SERVER DAEMON SYSLOGD [ENABLED] HOST1<ip-address-syslogd-host1>
                             [DISABLED]
```

For Host 2, use:

```
DEFINE SERVER DAEMON SYSLOGD [ENABLED] HOST2<ip-address-syslogd-host2>
                             [DISABLED]
```

Where	**Means**
ENABLED	Enable the syslogd daemon on the server. If you enable the daemon, you must also specify the Internet address of the remote host.
Host*n*	Specify either Host1 or Host2.
internet-address	The Internet address of the host where the destination log file resides.
DISABLED	Disable the syslogd daemon on the server. This is the default.

Example

```
DEFINE SERVER DAEMON SYSLOGD ENABLED HOST1 140.114.12.6
```

SET SERVER DATE — Privilege: P

Use this command to set or change the date maintained by the server. You cannot define the time because the server does not have an internal clock; therefore you will need to reset after each reboot.

Note that the load server (the host from which the server obtains software to run) supplies the default date that is maintained by the unit.

Syntax

SET SERVER DATE *dd mmm yyyy*

Where	Means
dd mmm yyyy	The new date which will be maintained by the unit. Specify this date using the following format: *dd* — a one or two digit number which is the day of the month. Valid values for dd are numbers in the range of 1 to 31. *mmm* — the first three letters of the month (e.g., JAN, FEB, etc). *yyyy* — is the year (e.g., 1993). Separate each item in the date with a space.

Example

```
SET SERVER DATE 03 OCT 1998
```

DEFINE/SET SERVER DUMP Privilege: P

Use this command to specify whether or not the server will perform a "crash dump" of the contents of the server memory, when the server detects a fatal error, before the server re-initializes.

During a crash dump procedure, the server sends a copy of the contents of its memory to a "dump file" at the load host for analysis by Xyplex Customer Support personnel, and the server re-initializes.

Syntax

```
DEFINE/SET SERVER DUMP      [DISABLED]
                            [ENABLED]
```

Where	Means
DISABLED	The server will not perform a memory dump when it detects a fatal error.
ENABLED	The server will perform a memory dump when it detects a fatal error. This is the default.

Example

```
DEFINE SERVER DUMP ENABLED
```

DEFINE SERVER DUMP PROTOCOL Privilege: P

The DEFINE SERVER DUMP PROTOCOL command enables or disables one or all dump protocols. The access server uses a dump protocol to send information to a dump server. All available dump protocols are enabled by default. This command is supported only on MAXserver Access Servers or Network 9000 Access Server 720.

Syntax

On MAXserver 1604/1608'/1620/1640 Access Servers or Network 9000/720 Access Server:

```
DEFINE SERVER DUMP record  PROTOCOL protocol [ENABLED]
                                             [DISABLED]
```

On MAXserver 800/1600 Access Servers or MAXserver 1450 Printer Server:

```
DEFINE SERVER DUMP PROTOCOL protocol   [ENABLED]
                                       [DISABLED]
```

Where	Means
record	One or more of the following initialization records: PRIMARY SECONDARY TERTIARY ALL The PRIMARY initialization record is the default.
protocol	One of the following protocols :

Protocol	Means
XMOP	Xyplex MOP Protocol
MOP	Digital Equipment Corporation Maintenance Operations Protocol
BOOTP	Bootstrap protocol
RARP	UNIX Reverse Address Resolution Protocol
ALL	All protocols

Note: Xyplex Access Servers cannot load from a DEC Info Server or any other device that does not support loading via DEC MOP V3 using all 5 parameters (Including the fifth parameter, which is the Host date/time stamp) for "Parameter Load with Transfer Address" using MOP.

ENABLED	Enable the protocol. You can enable only one protocol in the command line, unless you use the keyword ALL to enable all protocols.
DISABLED	Disable the protocol. You can specify ALL to disable all protocols.

Examples

1. This command enables BOOTP as a dump protocol for the primary record.

```
DEFINE SERVER DUMP PROTOCOL BOOTP ENABLED
```

2. This command disables XMOP as a dump protocol for the secondary record.

```
DEFINE SERVER DUMP SECONDARY PROTOCOL XMOP DISABLED
```

DEFINE/SET SERVER EVENTLOG Privilege: P

Use this command to control logging of events. This command is not supported on access servers that provide MANAGER services on memory cards. Use this command for MAXserver 1800/1820 or MAXMAN units only to record when certain events occur (for example, when it loads another unit, stores parameters or a dump from a unit, offers load/dump/parameter services, etc).

See the *Xyplex Loader Kits Guide* for more information about the event log.

Syntax

```
DEFINE SERVER EVENTLOG    [ENABLED]
                          [DISABLED]
```

Where	Means
ENABLED	Specifies that the unit will record when certain events occur. This is the default.
DISABLED	Specifies that the unit will not record when certain events occur.

Example

```
DEFINE SERVER EVENTLOG ENABLED
```

SET SERVER FORMAT CARD — Privilege: P

Use this command to format a flash card that can then be used to update the server parameters.

There is no Define command for this option.

CAUTION

This command deletes all data on the flash card.

Syntax

```
SET SERVER FORMAT CARD

SET SERVER FORMAT CARD OPTION <option n> [NONREDUNDANT]
```

Where	Means
OPTION	You will select a format option. See *Release Notes*.
option n	Select one of the following format options: 1 - 2 - 3 -
NONREDUNDANT	Disable redundant parameter file storage on the flash card.

Example

```
SET SERVER FORMAT CARD OPTION 2 NONRENDUNDANT
```

SET SERVER GET CARD Privilege: P

Use this command to initiate and terminate flash card load image updates. See also the GET CARD LOAD COMMAND for more information. Use the SHOW/MONITOR CARD STATUS Command to display the current settings.

There is no Define command for this option.

Syntax

```
SET SERVER GET CARD [LOADFILE] [“file-name”] IP ADDRESS [ip-address]AREA [area-number]
                                              ETHERNET ADDRESS [ether-address] AREA [area-number]
                    [STOP]
```

Where	Means
LOADFILE	Loads the image file.
"file-name"	The images file name. Enclose the name in quotes.
IP ADDRESS	Location of stored file to GET.
STOP	Terminates the file loading process.
ETHERNET ADDRESS	Location of the stored file to GET
AREA	The area on the card the image file is located in.

Example

```
SET SERVER GET CARD LOADFILE “xpcsrv20.sys” IP ADDRESS 140.179.192.110
```

DEFINE/SET SERVER HEARTBEAT Privilege: P

Use this command to enable or disable the Ethernet heartbeat signal on an access server.

Note: *Do not enable the Heartbeat feature if you are using a 10Base-T LAN connection.*

Syntax

```
DEFINE/SET SERVER HEARTBEAT    [ENABLED]
                               [DISABLED]
```

Where	Means
ENABLED	The access server will send out an Ethernet heartbeat signal.
DISABLED	The Ethernet heartbeat signal is disabled. This is the default.

Example

```
DEFINE SERVER HEARTBEAT ENABLED
```

DEFINE SERVER HELP — Privilege: P

Use this command to enable or disable the HELP facility. Some hardware types only offer reduced HELP messages.

You must reboot the server using the INIT DELAY command for the change to take effect.

Syntax

```
DEFINE SERVER HELP   [ENABLED]
                     [DISABLED]
```

Where	Means
ENABLED	Specifies that users will be able to obtain help information about commands via the HELP facility. This is the default.
DISABLED	Specifies that users will not be able to obtain help information about commands via the HELP facility.

Example

```
DEFINE SERVER HELP DISABLED
```

DEFINE/SET SERVER IDENTIFICATION Privilege: P

Use this command to specify a message identifying the server which is displayed on the SHOW SERVER screen.

Syntax

```
DEFINE/SET SERVER IDENTIFICATION "message-string"
```

Where	Means
message-string	The text that will be displayed, for identification purposes, in server displays. The identification message can be up to 40 ASCII characters long, and must be enclosed within quotation marks ("). To remove a previously specified identification message, enter a quoted null string (" "). The default is no identification message.

Example

```
DEFINE SERVER IDENTIFICATION "BOSTON SERVER"
```

DEFINE/SET SERVER IDENTIFICATION SIZE Privilege: P

Use this command to specify the maximum length of LAT node and service identification strings that the server stores in memory. (The server obtains these strings from service broadcasts from other nodes and displays them in SHOW/LIST/MONITOR NODES and SERVICES displays.) By changing the maximum length of LAT node and service identification strings, the user can reduce or eliminate the memory used for these identification strings, thus freeing memory for other uses.

See the Server Default Settings section in the *Configuration Guide* for more information on how to manage server resources.

Syntax

```
DEFINE/SET SERVER IDENTIFICATION SIZE size
```

Where	Means
size	The maximum size (bytes) of LAT node and service identification strings that are saved in server memory. Valid values for size are between 0 and 63. Specifying a value of 0 will prevent any node or service identification strings from being saved. The default value is 63.

Example

```
Xyplex>> DEFINE SERVER SERVER IDENTIFICATION SIZE 20
```

DEFINE SERVER IMAGE [LOAD] PROTOCOL Privilege: P

Use this command to enable or disable protocols used by the ROMs when the server attempts to load the image file. There is no SET command available for this feature.

Syntax

```
DEFINE SERVER IMAGE [LOAD] PROTOCOL <protocol>[ENABLED]
                                    [ALL]     [DISABLED]
```

Where	Means
ENABLED	Use this image load protocol.
DISABLED	Do not use this image load protocol
protocol	The image protocol the access server will use to load its image file. The valid values are CARD, XMOP, MOP, BOOTP, RARP, DFTP. The default setting is ALL. If you do not choose ALL, each protocol can be enabled one at a time.

Note: Xyplex Access Servers cannot load from a DEC Info Server or any other device that does not support loading via DEC MOP V3 using all 5 parameters (Including the fifth parameter, which is the Host date/time stamp) for "Parameter Load with Transfer Address" using MOP.

Examples

```
DEFINE SERVER IMAGE LOAD PROTOCOL RARP ENABLED

DEFINE SERVER IMAGE LOAD PROTOCOL ALL ENABLED
```

DEFINE/SET SERVER INACTIVITY TIMER Privilege: P

Ports are considered inactive while they are in the Local command mode, do not have any active sessions established, and there is no input, output, or modem transmission.

Use this command to specify for an entire server, how long inactive ports will remain logged on before the server will log them out. This setting only applies to inactive ports, that have the DEFINE/SET PORT INACTIVITY LOGOUT enabled.

Syntax

```
DEFINE/SET SERVER INACTIVITY TIMER time
```

Where	Means
time	Specifies the length of time for which a port can remain inactive, before that port is logged out. The valid values are between 1 and 120 minutes. The default is 30 minutes.

Example

```
DEFINE SERVER INACTIVITY TIMER 20
```

DEFINE/SET SERVER INTERNET OR IP Commands

Use the SERVER INTERNET or IP commands to modify Internet-related access server settings in the operational database.

See the following server-related internet commands for more information

```
DEFINE/SET IP ADDRESS
DEFINE/SET IP BROADCAST ADDRESS
DEFINE/SET IP DEFAULT DOMAIN SUFFIX
DEFINE/SET IP DOMAIN TTL
DEFINE/SET IP NAME
DEFINE/SET IP PRIMARY DOMAIN ADDRESS
DEFINE/SET IP FILTER
DEFINE/SET IP GATEWAY TIMEOUT
DEFINE/SET IP PRIMARY GATEWAY ADDRESS
DEFINE/SET IP ROTARY
DEFINE/SET IP ROUTE
DEFINE/SET IP SECONDARY DOMAIN ADDRESS
DEFINE/SET IP SECONDARY GATEWAY ADDRESS
DEFINE/SET IP SNMP
DEFINE/SET IP SUBNET MASK
DEFINE/SET IP SUBNET MASK AUTOCONFIGURE
DEFINE/SET IP TCP CONNECT TIMER
DEFINE/SET IP TCP RETRANSMIT
DEFINE/SET IP TRANSLATION TABLE TTL
DEFINE/SET IP TTL
```

DEFINE/SET SERVER IP ADDRESS Privilege: P

Use this command to specify the Internet address for this server. You cannot SET this parameter while there are active Telnet sessions on this server.

This command requires that the Telnet protocol be enabled. It is not supported on LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units which support Telnet or are LAT-only units).

Syntax

DEFINE/SET SERVER IP ADDRESS *internet-address*

Where	Means
internet-address	The Internet addressfor this server. The default value is 0.0.0.0 (no internet-address).

Example

```
DEFINE SERVER IP ADDRESS 140.179.224.100
```

DEFINE SERVER IP ADDRESS AUTODISCOVERY Privilege: P

Use this command to allow the server to acquire its working IP address in a non-standard method. Use the SHOW/LIST SERVER IP CHARACTERISTICS command to display the new parameter. If you enable autodiscovery, the server will be able to obtain its working IP address even if loading is done using non-standard methods.

The following scenarios describe the results of using auto discovery.

Reboot the server using the INIT DELAY command in order for these changes to take effect.

Scenario 1:

You load an image using BOOTP, load the parameter file using BOOTP or NVS, and use an IP address defined in the ROM menu.

Result:

After bootup, the server will send out a BOOTP request for an IP address and will take on that address as its working IP address.

Scenario 2:

Load an image using BOOTP, your parameters through NVS and use the IP address defined in the ROM menu.

Result:

After bootup, the access server will send out a BOOTP request for an IP address. If there is no response to the BOOTP request, five additional BOOTP requests (one per minute) will be sent. If a response is received, then that IP address will be used as the server's working address. If there is no response in the allotted time, then the server will use the IP address defined in the parameter file, or if there is no address in the parameter file, the server will use the IP address defined in the BOOTPTAB file from the BOOTP load image server as its working IP address.

Scenario 3:

Load image through a non-BOOTP method, load parameter file from NVS and the IP address defined in the ROM menu.

DEFINE SERVER IP ADDRESS AUTODISCOVERY (continued)

After bootup, the server will send out a BOOTP request for an IP address. If there is no response within the alotted time (see previous scenario), then the IP address is defined in the parameter file. If there is no address defined in the parameter file, then the server will use the IP address defined in the ROM menu as its working IP address. If there is no IP address defined in the ROMs, then the server will send out BOOTP requests at 1-minute intervals until it gets a BOOTP response.

Syntax

```
DEFINE SERVER IP ADDRESS AUTODISCOVERY [ENABLED]
                                       [DISABLED]
```

Where	Means
ENABLED	Allows the autodiscovery of the IP address.
DISABLED	Address cannot be located using autodiscovery. This is the default.

Example

```
DEFINE SERVER IP ADDRESS AUTO DISCOVERY ENABLED
```

DEFINE/SET SERVER IP BROADCAST ADDRESS Privilege: P

Specifies that you will define or change the Internet address of the server that is used in Internet Broadcast messages. You cannot change this parameter while there are active Telnet terminal sessions on this server.

This command requires that the Telnet protocol is enabled. It is not supported on LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units that support Telnet or are LAT-only units).

Syntax

```
DEFINE/SET SERVER IP BROADCAST ADDRESS internet-address
```

Where	Means
internet-address	Specifies the Internet address of this server that is used in Internet Broadcast messages. The default value is 255.255.255.255.

Example

```
DEFINE SERVER IP BROADCAST ADDRESS 255.255.255.0
```

DEFINE/SET SERVER IP DEFAULT DOMAIN SUFFIX Privilege: P

Use this command to specify the default *domain-name-suffix* specification(s). The server uses the value(s) that you specify for the default *domain-name-suffixes* to develop a complete (fully-qualified) *domain-name*, whenever the user specifies an incomplete *domain-name*. (See the section listing **Common Variables** at the beginning of this book for a definition of *domain names*.)

When only a single default *domain-name-suffix* is specified, and a user specifies a *domain-name* that does not contain a period in a SHOW, LIST, CLEAR, PURGE, SET, or DEFINE SERVER IP DOMAIN command, the software appends the default *domain-name-suffix* to the user-specified name. However, if multiple *domain-name-suffixes* are specified, the software will qualify the given name only with the first default *domain-name-suffix* specified by the IP DEFAULT DOMAIN SUFFIX characteristic. Therefore, you should specify the most frequently used suffix as the first one in the list.

This command requires that the Telnet protocol be enabled. It is not supported on LAT-only units (refer to the *Software Kit Information* supplied on your CD for a list of units that support Telnet or are LAT-only units).

Syntax

```
DEFINE/SET SERVER IP DEFAULT DOMAIN SUFFIX        [suffix-list]
                                                  [NONE]
```

where the *suffix-list* syntax is:

```
[domain-name-suffix1|domain-name-suffix2| ...|domain-name-suffix8]
```

Where	Means
domain-name-suffix1 through *domain-name-suffix8*	The domain-name suffix that the server will use to develop a complete (fully-qualified) domain-name, whenever a user specifies an incomplete domain-name. The server appends the suffix to the incomplete domain-name. Specify domain-name-suffixes beginning with a period character (.). The domain-name-suffixes cannot end with a period. Do not enclose the name in quotation marks. Separate each domain-name suffix with the vertical bar character (|) and no spaces. The default value for this setting is the null value. The maximum total characters of all names together, including vertical bars '|' and periods '.', cannot exceed 115 characters. The entire command line cannot exceed 132 characters. Each domain-name is limited to a maximum of 50 characters. One of the suffixes can be "no suffixes" which is specified by a single period. The keyword NONE indicates no suffixes.

Examples

Suffix domain list:

```
DEFINE SERVER IP DEFAULT DOMAN SUFFIX  .|.XYPLEX.COM|.NBASE.COM
```

Single domain:

```
DEFINE SERVER IP DEFAULT DOMAIN SUFFIX .|.COM
```

DEFINE/SET SERVER IP DOMAIN ADDRESS Privilege: P

Use this command to specify the internet address where a Domain name server is located. (Domain name servers are network objects where the network attempts to resolve a domain-name.) The server can use up to two Domain name servers (primary and secondary) to resolve a domain-name. The server will query all designated Domain servers to resolve a domain-name.

This command requires that the Telnet protocol is enabled. It is not supported on LAT-only units (refer to the *Software Kit Information* supplied on the CD for a list of units which support Telnet or are LAT-only units).

Syntax

```
DEFINE/SET SERVER INTERNET [PRIMARY] DOMAIN ADDRESS internet-address
DEFINE/SET SERVER INTERNET [SECONDARY] DOMAIN ADDRESS internet-address
```

Where	Means
internet-address	The address of the primary or secondary Domain name server. The default value is 0.0.0.0 (no Domain name server) You can use the same value for the IP DOMAIN ADDRESS and the IP BROADCAST ADDRESS. If you do, then other servers will respond to Domain name requests for their Internet name by supplying their internet-address.
PRIMARY	The Domain name server at the internet-address is the primary Domain name server.
SECONDARY	The Domain name server at the internet-address is the secondary Domain name server

Example

```
DEFINE SERVER IP PRIMARY DOMAIN ADDRESS 140.179.224.100
```

DEFINE SERVER IP HOST

Use this command to specify the host's IP address that will be used as the TFTP LOAD HOST to download the software image. Use the LIST SERVER LOADDUMP CHAR command to display the current setting.

The SET command is not available for this option.

DEFINE SERVER INTERNET IP REASSEMBLY Privilege: P

Use this command to control whether or not server will attempt to reassemble fragmented TCP/IP packets that it receives.

Sometimes, packets that are forwarded by a gateway or a router become fragmented between the source and the destination (i.e., the server). Generally, packet fragmentation is not a problem, but when it is, the server can either attempt to reassemble the fragmented packets, or it can simply discard them. Packet fragmentation can cause problems, particularly when using protocols that do not include a resend mechanism (such as UDP, which does not guarantee that data will be received successfully).

Enabling this command requires additional server memory resources, because the server must store all the fragments until it can reassemble the complete packet. In this case, you may need to increase the setting for the DEFINE/SET SERVER PACKET BUFFER. If the server has limited extra memory, or when packet fragmentation is not a frequent problem, it is recommended that you disable SERVER IP IP REASSEMBLY.

Syntax

```
DEFINE SERVER INTERNET IP REASSEMBLY    [ENABLED]
                                        [DISABLED]
```

Where	Means
ENABLED	The server will attempt to reassemble fragmented TCP/IP packets that it receives.
DISABLED	The server will not attempt to reassemble fragmented TCP/IP packets that it receives, and the server will discard the fragments. This is the default.

Example

```
DEFINE SERVER INTERNET IP REASSEMBLY ENABLED
```

DEFINE/SET SERVER IP LOAD FILE Privilege: P

Use this command to specify the name of the file that will be requested upon a boot up when loading from a TFTP server. Use the LIST SERVER LOADDUMP CHARACTERISTICS command to display the current file name.

Syntax

```
DEFINE SERVER IP LOAD FILE “message-string”

DEFINE SERVER IP FILE “message-string”
```

Item	Description
“*string*”	Specify a filename of up to 64 characters. Use the quotation marks “ “ before and after the file name. The default is an empty field.

Example

```
DEFINE IP LOAD FILE “filename.sys”
```

DEFINE/SET SERVER INTERNET NAME Privilege: P

Use this command to specify the domain-name by which the server is known on the network.

This command requires that the Telnet protocol is enabled. It is not supported on LAT-only units (refer to the *Software Kit Information* supplied on your CD for a list of units which support Telnet or are LAT-only units).

Syntax

```
DEFINE/SET SERVER INTERNET NAME <domain-name>
```

Where	Means
domain-name	The domain-name by which the server is known on the network. The specified domain-name must be a fully qualified domain-name (the specified name will not be concatenated with any default Internet domain-name-suffixes).

Example

```
DEFINE SERVER INETRNET NAME SERVER1.XYPLEX.COM
```

DEFINE/SET SERVER IP DELIMITER Privilege: P

Use this command to specify the file delimiter used by the host system to determine directory boundaries. Use the LIST SERVER LOADDUMP CHAR command to display the current delimiter setting.

Syntax

```
DEFINE SERVER IP DELIMITER [“string”]
```

Where	Means
message-string	Specify the file delimiter such as "\" or "/" that the host uses as a file delimiter. For example, DOS (PC) uses \ while UNIX uses /.

Example

```
DEFINE SERVER IP DELIMITER "/"
```

DEFINE/SET SERVER IP DOMAIN TTL Privilege: P

When Domain Name Servers respond to a request for a domain-name that is made by the server, the response includes a time-to-live (TTL) value, which indicates for how long the server should consider the domain-name to be valid.

Use this command to specify a maximum time-to-live (TTLvalue for all *domain names* learned by the server (i.e., override the TTL supplied by the Domain Name Server).

Requires that the Telnet protocol is enabled. It is not supported on LAT-only units (refer to the *Software Kit Information* supplied on your CD for a list of units which support Telnet or are LAT-only units).

Syntax

```
DEFINE/SET SERVER IP DOMAIN TTL  [time]
```

Where	Means
time	The number of hours (0 - 168) domain names are to be kept. All domain name responses that the server receives are assigned this value. If you enter zero (0), the TTL value supplied by the domain name server found will be used. If you enter a value greater than 168, an error message is displayed. The default value is 64.

Example

```
DEFINE SERVER IP DOMAIN TTL 24
```

Use the following commands to define IP traffic filters. Note that the Define/Set Server commands affect packets that the server receives from the attached LAN. The Define/Set Port commands affect packets received through individual ports.

If a server receives a packet that has multiple matching filters, the server applies the most specific filter. See the Using TCP/IP features section in the *Advanced Configuration Guide* for more information.

Note: Before you define filtering criteria for the server, you must have entered the DEFINE IP FILTERING ENABLED command to enable filtering on the server.

IP Traffic Filter Criteria

You can specify the following criteria in an IP traffic filter:

- IP protocol type: specific protocol ID number, TCP, UDP, or ALL
- Destination IP address and subnet mask
- Destination port number or range of numbers
- Source IP address and subnet mask
- Source port number or range of numbers
- Whether a TCP packet has its SYN bit ON and its ACK bit OFF

The commands to enable these IP traffic filters are described on the following pages.

Syntax

```
DEFINE/SET SERVER IP FILTER criteria-instructions

DEFINE/SET PORT port-list IP FILTER criteria-instructions
```

See the DEFINE/SET PORT commands to define port-level filtering.

DEFINE/SET SERVER IP FILTER DESTINATION Privilege: P

Use this command to define the IP traffic destination. Defining a destination allows or restricts traffic to or from the defined destination.

Syntax

```
DEFINE/SET SERVER IP FILTER DESTINATION [ip-address] [MASK subnet-mask]
                                                                [DISCARD]
                                              [ALL]             [FORWARD]

DEFINE/SET SERVER IP FILTER DESTINATION PORT [port number]  [DISCARD]
                                                            [ALL]
```

Where	Means
ip-address	The destination IP address.
MASK	The destination port's MASK and subnet mask. If the keyword MASK is omitted, the default mask characteristic (Natural Class mask) is used.
subnet-mask	The portion of an Internet address that refers to the remote network. Specify the *subnet-mask* using the same format as an Internet address, with ones for the network portion. (Note, if you do not specify a *subnet-mask* for an internet route entry, the software will automatically specify the *subnet-mask* based on the *internet-address.*
port number	The destination's port number or range of port numbers. The valid port numbers are 0 to 65535.
ALL	All destinations. This is the default setting.
DISCARD	Do not allow communication to the specified destination.
FORWARD	Allow communication to the specified destination.

Examples

```
DEFINE SERVER IP FILTER DESTINATION 192.168.22.105 MASK DISCARD

DEFINE SERVER IP FILTER DESTINATION PORT 5 FORWARD
```

DEFINE/SET SERVER IP FILTERING Privilege: P

Use this command to enable IP traffic filters on a server. If you do not enable filtering on the server no other filter commands will be acknowledged. Once IP filtering is enabled, the server then allocates memory to filtering.

Use the INIT DELAY command to reboot the server in order for the changes to take effect.

See the Using TCP/IP Features section in the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE SERVER IP FILTERING [ENABLED]
                           [DISABLED]
```

Where	Means
ENABLED	Activates IP traffic filtering on the server.
DISABLED	No filtering is allowed. This is the default.

DEFINE/SET SERVER IP FILTER PROTOCOL Privilege: P

Use this command to specify the IP protocol type for the server. See the Using TCP/IP Features section in the *Advanced Configuration Guide* for detailed information about how the server determines the most specific filter.

Syntax

```
DEFINE/SET SERVER IP FILTER PROTOCOL   [protocol-id]          [DISCARD]
                                       [TCP]                 [FORWARD]
                                       [UDP]
                                       [ALL]
```

Where	Means
protocol-id	The TCP or UDP Protocol ID number. A port number from 0 to 255.
TCP	Sets the IP protocol type to TCP.
UDP	Sets the IP protocol type to UDP.
ALL	Sets the IP protocol type to ALL. This is the default setting.
DISCARD	Any protocol which meets this criteria will not be forwarded.
FORWARD	Any protocol which meets this criteria will be forwarded.

Example

```
DEFINE SERVER IP FILTER PROTOCOL TCP DISCARD
```

DEFINE/SET SERVER IP FILTER SOURCE Privilege: P

Use this command to specify the IP sources that can communicate through the server's ports. You can set up the source filter for the entire server or on a per-port basis.

Syntax

```
DEFINE/SET SERVER IP FILTER SOURCE [ip-address [MASK subnet-mask]][DISCARD]
                                   [ALL]                          [FORWARD]

DEFINE/SET SERVER IP FILTER SOURCE PORT  [port number]            [FORWARD]
                                        [ALL]                     [DISCARD]
```

Where	Means
ip-address	The source IP address.
MASK	The source's MASK and subnet mask. If the keyword MASK is omitted, the default mask characteristic (Natural Class mask) is used.
subnet-mask	The portion of an Internet address that refers to the remote network. Specify the *subnet-mask* using the same format as an Internet address, with ones for the network portion. (Note, if you do not specify a *subnet-mask* for an internet route entry, the software will automatically specify the *subnet-mask* based on the *internet-address.*
port number	The source port number or a range of port numbers. The valid port numbers are 0 to 65535.
ALL	All sources. This is the default setting.
DISCARD	Do not allow communication to the specified source.
FORWARD	Allow communication to the specified source.

Examples

```
DEFINE SERVER IP FILTER SOURCE 140.179.240.1 FORWARD

DEFINE SERVER IP FILTER SOURCE PORT 5-8 DISCARD
```

DEFINE/SET SERVER IP FILTER SYN — Privilege: P

Use this command to allow or restrict the forwarding of TCP packets.

Syntax

```
DEFINE/SET SERVER IP FILTER SYN  [ON]           [DISCARD]
                                 [ALL]          [FORWARD]
                                 [OFF]
```

Where	Means
ON	The SYN (synchronization) bit is set to ON and the ACK (acknowledge) bit is set to OFF in the TCP header. This indicates that the sender is trying to open a new session with a destination port. By discarding packets with this bit pattern, you prevent remote users from opening sessions with hosts on the local network.
OFF	The SYN bit is set to OFF and the ACK bit is set to OFF in the TCP header.
ALL	Any value for the SYN and ACK bits. This is the default.
DISCARD	Prevent remote users from opening sessions with hosts on the local network.
FORWARD	Allow remote users to open sessions with hosts on the local network.

Example

```
DEFINE SERVER IP FILTER SYN ON DISCARD
```

DEFINE/SET SERVER IP GATEWAY ADDRESS Privilege: P

Use this command to specify an internet gateway address for the server. The server can use up to two Internet gateway routers (primary and secondary) to locate a device on an external network. The server will use the primary gateway to route a transmission to a remote device until it determines that the gateway has been unable to route the transmission successfully. Then it will use the secondary gateway.

This command requires that the Telnet protocol is enabled.

Syntax

```
DEFINE/SET SERVER IP [PRIMARY] GATEWAY ADDRESS <internet-address>
                    [SECONDARY]
```

Where	Means
internet-address	The internet address of the primary or secondary internet gateway. The default value is 0.0.0.0 (no gateway).
PRIMARY	Internet-address specified is for the primary Internet gateway router.
SECONDARY	Internet-address specified is for the secondary Internet gateway router.

Example

```
Xyplex>> DEFINE SERVER IP PRIMARY GATEWAY ADDRESS 140.179.224.100
```

DEFINE/SET SERVER IP GATEWAY TIMEOUT Privilege: P

This command lets you specify how often (in seconds) the primary gateway is ping'd to determine its status. The time set also determines how often the server will switch between the primary and secondary gateways.

Use the SHOW SERVER IP command to display the current value of this command.

Syntax

```
XYPLEX> DEFINE SERVER IP GATEWAY TIMEOUT <number-of-seconds>
```

Item	Description
number-of-seconds	Specify how often the server will switch between the primary and secondary gateways. The valid values are 1 to 300 seconds. The default is 60 seconds.

DEFINE/SET SERVER IP NAME Privilege: P

Use this command to define the server's IP name. This name can be a domain name. Use the SHOW SERVER IP CHAR command to display the current Domain Name setting.

SYNTAX

```
DEFINE/SET SERVER IP NAME [domain-name]
```

Where	Means
domain-name	The server's system name. This is the name which the server is identified. The name must contain at least one period (.).

Example

```
DEFINE SERVER IP NAME XYPLEX.COM
```

DEFINE/SET SERVER IP LOCAL BASE Privilege: P

Use this command to define the local TCP port starting base for the server as well as an optional increment value. The base value is used as the local TCP port for Port 0. Each subsequent port's local TCP port is calculated as:

(*port number* * *increment-value*) +*base-value*

Syntax

```
DEFINE/SET SERVER IP LOCAL BASE [base-value] [INCREMENT increment-value]
```

Where	Means
base-value	A value from 1 to 32767. The default value is 4000.
increment-value	A value from 1 to 1024. The default value is 100.
INCREMENT	Specifies a change to the *increment-value.* If this keyword is not included on the command line, the *increment-value* remains unchanged.

Example

```
DEFINE SERVER IP LOCAL BASE 3000 INCREMENT 200
```

DEFINE/SET SERVER IP ROTARY Privilege: P

The term "rotary" refers to the ability to assign the same internet-address or domain-name to multiple ports that offer the same type of service.

Use this command to create a rotary by assigning an internet address to one or more ports on the same server. See the Port Settings section in the *Configuration Guide* for information about Configuring Rotary Connections.

This command requires that the Telnet protocol is enabled.

Syntax

```
DEFINE/SET SERVER IP ROTARY   [internet-address port-list]
                              [domain-name port-list]
```

Where	Means
internet-address	The internet address that will be assigned to the port(s) in the port-list.
domain-name	The domain name that will be assigned to the port(s) in the port-list.
port-list	The port(s) to which the internet address or domain name will be assigned.

Example

```
DEFINE SERVER IP ROTARY PRINTER.XYPLEX.COM 2-4
```

DEFINE/SET SERVER IP ROUTE Privilege: P

An internet route specifies the preferred gateway on the local network to which the server should route traffic on the way to a particular destination host or network. The server contains a list of internet routes in both the operational and permanent databases. This list is called a routing table.

See the Using the TCP/IP Features section in the *Advanced Configuration Guide.*

Use this command to add internet route entries to the operational or permanent routing table. Internet routes that are entered into the databases via a DEFINE/SET SERVER IP ROUTE commands are called locally defined internet-routes.

In addition to the locally defined internet routes, the server can use internet-routes that it obtains from one or more Internet gateways in the network. These internet-routes are only entered into the operational database. Internet-routes that are entered into the databases via a Internet gateway are called "learned" internet-routes. The server retains a learned internet-route in the operational database until one of the following occurs:

- It is removed via a CLEAR SERVER IP ROUTE command.
- The period of time (time to live) that is assigned by the Internet gateway expires. The TCP/IP-LAT software limits the time to live to a maximum of 1 week (168 hours).
- The operational database contains the maximum number of internet-routes, a user adds a new internet route via a SET SERVER IP ROUTE command, or the access server learns a new internet-route from an Internet gateway. In this case, the unit replaces the oldest learned internet-route in the operational database with the new internet-route.

Internet routes that are listed in the permanent database are entered into the operational database whenever the access server is re-initialized. Internet-routes that are listed in the permanent database remain until they are deleted by a PURGE SERVER IP ROUTE command.

The operational and permanent databases can contain a maximum of 64 internet-routes by default. Locally defined internet-routes remain in the operational database until they are removed via a CLEAR SERVER IP ROUTE command.

This command requires that the Telnet protocol is enabled. It is not supported on LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units which support Telnet or are LAT-only units).

Syntax

`DEFINE/SET SERVER IP ROUTE` *`int-addr`* `GATEWAY` *`gateway-int-addr network-options`*

Use the following syntax for the *network-options*:

```
[Network]   [Mask subnet-mask]   [Fixed]
                                 [Variable]
[Host]                           [Fixed]
                                 [Variable]
```

Where	Means
int-addr	The address of the destination host or the address from which the access server should derive the address of the network on which a host is located. Use the standard internet-address format.
GATEWAY	The gateway-internet-address which follows is the address of the gateway which will forward network traffic to the destination specified by the internet-address.
gateway-int-addr	The internet-address of the gateway which will forward network traffic to the destination specified by the internet-address. Specify using the standard internet-address format. The gateway-internet-address must be on the local network.
Network	The access server should use the internet-address to determine the destination network. This is the default.
Host	The access server should interpret the internet-address as being the address of a host.
Mask	You will define the Internet *subnet-mask* for the routing table network entry (i.e., cannot be used in conjunction with the HOST keyword). The purpose of a subnet mask is to identify which portion of an Internet address refers to the remote network.
subnet-mask	The portion of an Internet address that refers to the remote network. Specify the *subnet-mask* using the same format as an Internet address, with ones for the network portion. (Note, if you do not specify a *subnet-mask* for an internet route entry, the software will automatically specify the *subnet-mask* based on the *internet-address.*
Fixed	The access server cannot modify this internet route entry based on the information contained in ICMP routing messages that it receives. This is the default.
Variable	The access server can modify this internet route entry based on the information contained in ICMP routing messages that it receives.

Examples

```
DEFINE SERVER IP ROUTE 192.12.120.255 GATEWAY 128.6.201.7
```

Meaning: Assume that you are on a access server which has the internet address 128.6.201.4. Since the NETWORK characteristic is the default, the access server uses the *internet-address* to determine that all network traffic to the class C network 192.12.120.0 is routed to the gateway at internet address 128.6.201.7. This internet-route entry is added to the permanent database.

```
SET SERVER IP ROUTE 130.12.255.255 GATEWAY 128.6.201.8
```

Meaning: Assume that you are on a access server which has the internet address 128.6.201.4. In this example, all traffic to the class B network 130.12 is routed to the gateway at internet address 128.6.201.7. This internet-route entry is added to the temporary database.

```
SET SERVER IP ROUTE 192.12.120.21 GATEWAY 128.6.201.8 HOST
```

Meaning: Assume that you are on a access server which has the internet address 128.6.201.4. In this example, all traffic to the host at internet address 192.12.120.21 is routed through the gateway at internet address 128.6.201.8. This internet-route entry is added to the temporary database.

```
SET SERVER IP ROUTE 192.16.63.255 GATEWAY 128.6.201.8 MASK 255.255.255.00
```

Meaning: Assume that you are on a access server which has the internet address 128.6.201.4. In this example, the access server will route all traffic to the network address C0.10.3X.XX (a hexadecimal representation of the internet address 192.16.63.255 ANDed with the subnet-mask 255.255.255.00, and where hexadecimal numbers show the network portion of the internet address and the letter X represents the host portion of the internet address) to the gateway at internet address 128.6.201.8. This internet-route entry is added to the temporary database.

DEFINE SERVER IP ROUTING TABLE SIZE Privilege: P

An Internet route specifies the preferred gateway on the local network where the server can route traffic bound for a particular destination. The server contains a list of Internet routes in both the operational and permanent databases. This list is called a routing table.

You can increase or decrease the number of Internet routes that can be stored in the operational Internet routing table. The operational Internet routing table contains all statically defined and learned Internet routes. This table can contain between 64 and 512 entries. The maximum size of the permanent Internet routing table, which contains a list of permanent statically defined Internet routes, has a default size of 64 entries.

Note: *Prior to version 5.3.1 , the size of the Internet routing table was fixed and the table could store a maximum of 64 entries (one entry for each Internet route stored).*

Use this command to specify the size of the operational Internet routing table. You must reboot the server using the INIT DELAY command in order for the change to take effect.

Syntax

```
DEFINE SERVER IP ROUTING TABLE SIZE table-size
```

Where	Means
table-size	The maximum number of learned and static Internet routes that the operational Internet routing table can contain. The *table-size* can be from 64 to 512 entries. The default is 64 entries.

Example

```
DEFINE SERVER IP ROUTING TABLE SIZE 256
```

DEFINE SERVER IP SECURITY Privilege: P

Use this command to enable or disable the IP Security feature so that Telnet connections can be either allowed or denied between specified ports on the server and specific internet-addresses. The PORT IP SECURITY setting specified for the individual port determines whether the connection is allowed or denied. Enabling this feature only allows the feature to be available.

See the Security Features section of the *AdvancedConfiguration Guide* for more information.

This command requires that the Telnet protocol is enabled.

You must reboot the server using the INIT DELAY command in order for the change to take effect.

Syntax

```
DEFINE SERVER IP SECURITY        [ENABLED]
                                 [DISABLED]
```

Where	Means
ENABLED	Telnet connections can be either allowed or denied between specified ports on the server and specific internet-addresses (via the PORT IP SECURITY setting).
DISABLED	Telnet connections cannot be allowed or denied between specified ports on the server and specific internet-addresses (via the PORT IP SECURITY setting. This is the default.

Example

```
Xyplex>> DEFINE SERVER IP SECURITY DISABLED
```

DEFINE/SET SERVER IP SNMP AUTHENTICATION TRAPS Privilege: P

Use this command to allow Authentication traps to be sent. The default is Enabled. Use the SHOW SERVER IP SNMP command to display the current settings.

Syntax

```
DEFINE SERVER IP SNMP AUTHENTICATION TRAPS [ENABLED]
                                           [DISABLED]
```

Item	Description
ENABLED	Allows authentication traps to be sent. This is the default setting.
DISABLED	Prevents authentication traps from being sent.

DEFINE/SET SERVER IP SNMP CLIENT Privilege: P

Use this command to add an SNMP client.

When an SNMP community name has been specified for the unit, any SNMP clients that you specify must belong to the same community as the unit, in order for the clients to be able perform an SNMP set on a unit.

When you have not specified an SNMP Set or Get community name or any SNMP clients for the unit, the unit will accept SNMP set or get commands from any client. No traps are transmitted if there are no SNMP Trap clients.

The Telnet protocol must be enabled before you can define the SNMP settings.

Non-supported Products

SNMP is not supported on the following products:

- LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units which support Telnet or are LAT-only units).
- MAXserver 1400 Network Printer Server
- MX-TSERV-J8 and MX-TSRVL-J8 cards.

Use the SHOW SERVER IP SNMP CHARACTERISTICS command to display the current SNMP settings. For more information, see the SNMP settings section of the *Advanced Configuration Guide*.

Syntax

```
DEFINE/SET SERVER IP SNMP [GET CLIENT client-number internet-address]
                          [SET CLIENT client-number internet-address]
                          [TRAP CLIENT client-number internet-address]
```

DEFINE/SET SERVER IP SNMP CLIENT (continued)

Where	Means
GET CLIENT	Add or change the SNMP clients (e.g., a Network Operations Center, or NOC) that have permission to view information about the unit (i.e., perform an SNMP get). You can define up to 12 clients.
SET CLIENT	Add or change the SNMP clients (e.g., a Network Operations Center, or NOC) that have permission to set characteristics (i.e., perform an SNMP set) on the unit. You can define up to 12 clients.
TRAP CLIENT	Add or change the SNMP clients (e.g., a Network Operations Center, or NOC) that will receive SNMP traps generated by the unit. You can define up to 12 clients.
client-number	The number of the SNMP client that has permission to set characteristics (i.e., perform an SNMP set) on the unit, to view information about the unit (i.e., perform an SNMP get), or to receive SNMP traps generated by the unit. Valid values are 1, 2, 3, and 4.
internet-address	The internet-address of an SNMP client has permission to set characteristics (i.e., perform an SNMP set) on the unit, to view information about the unit (i.e., perform an SNMP get), or receive SNMP traps generated by the unit. The default value is 0.0.0.0. Specify the default value to remove a client.

Example

```
DEFINE SERVER IP SNMP GET CLIENT 2 0.0.0.0
```

DEFINE/SET SERVER IP SNMP COMMUNITY Privilege: P

Use this command to add an SNMP community.

When an SNMP community name has been specified for the unit, any SNMP clients which you specify must belong to the same community as the unit, in order for the clients to be able perform an SNMP set on a unit.

When you have not specified an SNMP Set or Get community name or any SNMP clients for the unit, the unit will accept SNMP set or get commands from any client. No traps are transmitted if there are no SNMP Trap clients.

The Telnet protocol must be enabled before you can define the SNMP settings.

Non-supported Products

SNMP is not supported on the following products:

- LAT-only units (refer to the *Software Kit Information* supplied on your CD for a list of units that support Telnet or are LAT-only units).
- MAXserver 1400 Network Printer Server
- MX-TSERV-J8 and MX-TSRVL-J8 cards.

Use the SHOW SERVER IP SNMP CHARACTERISTICS command to display the current SNMP settings. For more information, see the SNMP settings section of the *Advanced Configuration Guide*.

Syntax

```
DEFINE/SET SERVER IP SNMP [GET COMMUNITY] [community-name]
                                          [NONE]
                          [SET COMMUNITY]  [community-name]
                                          [NONE]
                          [TRAP COMMUNITY] [community-name]
```

DEFINE/SET SERVER IP SNMP COMMUNITY (continued)

Where	Means
GET COMMUNITY	Add or change the name of the SNMP Get community to which the unit belongs. When a community name has been specified for the unit, only SNMP Get clients (e.g., a Network Operations Center, or NOC)that belong to the same Get community are permitted to view information about the unit (i.e., perform an SNMP get).
SET COMMUNITY	Add or change the name of the SNMP Set community to which the unit belongs. When a community name has been specified for the unit, only SNMP Set clients (e.g., a Network Operations Center, or NOC) that belong to the same Set community are permitted to set characteristics (i.e., perform an SNMP set) on the unit.
TRAP COMMUNITY	Add or change the name of the SNMP Trap community to which the unit belongs. When a community name has been specified for the unit, only SNMP Trap clients (e.g., a Network Operations Center, or NOC) that belong to the same Trap community will receive SNMP traps which are generated by the unit. The default community name is "public"
"*community-name*"	The name of the SNMP Get, Set, or Trap community to which the unit belongs. The can be up to 32 characters long. The name is not case sensitive. Enclose the name within quotation marks ("). The string "public" is default for the Trap community. To clear the Trap community, use the null string ("").
None	The unit will not verify that SNMP clients belong to the same SNMP Get or Set community as the unit. This is the default for the Get and Set community. This keyword does not apply for the Trap community.

Example

```
DEFINE/SET SERVER IP SNMP GET COMMUNITY “XYPLEX”
```

DEFINE/SET SERVER IP SNMP SYSTEM CONTACT/LOCATION Privilege: P

Use the SYSTEM CONTACT command to supply the name of the person to contact when the access server needs attention. Use the SYSTEM LOCATION command to supply the access server's location.

Use the SHOW SERVER IP SNMP CHARACTERISTICS command to display the current SNMP settings.

Syntax

```
DEFINE/SET SERVER IP SNMP [SYSTEM CONTACT]   [contact-name]

DEFINE/SET SERVER IP SNMP [SYSTEM LOCATION]  [location-name]
```

Where	Means
IP SNMP System Contact	The name of a system contact for the unit. This information is available via an SNMP query (get) but is provided for administrative or informational purposes only.
contact-name	The name of a system contact for the unit. The name can be up to 60 characters. Enclose the string in quotation marks ("), and do not leave spaces. To remove a previously specified system contact name, enter a quoted null string (" ") for the name. The default value for this setting is "" (i.e., the null value).
IP SNMP System Location	The location of the unit. This information is available via an SNMP query (get) but is provided for administrative or informational purposes only.
location	The location of the unit. The location can be up to 60 characters. Enclose the string in quotation marks ("), and do not leave spaces. To remove a previously specified system location, enter a quoted null string (" ") for the name. The default value for this setting is "" (i.e., the null value).

Example

```
DEFINE/SET SERVER IP SNMP SYSTEM CONTACT  “John Smithson”

DEFINE/SET SERVER IP SNMP SYSTEM LOCATION “Closet1_Bldg2”
```

DEFINE/SET SERVER IP SUBNET MASK Privilege: P

Use this command to specify the IP subnet-mask for the server. The server uses the subnet mask to distinguish between IP addresses that can be reached directly from those that must be reached via an IP Gateway. Each device running TCP/IP protocols contains a subnet mask. When a user attempts to form a TCP/IP connection with a destination Internet node, the destination Internet address is logically ANDed with the subnet mask. The unit's own Internet address is also logically ANDed with the subnet mask.

The two results of these operations are compared. If they are equal, then the destination is assumed to be reachable without the assistance of an IP Gateway. If they are not equal, then the unit will attempt to reach the destination via an IP Gateway.

Make sure that Telnet protocol is enabled before you complete this command.

To use the IP Address Autoconfigure feature, you must disable this feature.

Syntax

```
DEFINE/SET SERVER IP SUBNET MASK [ip-address-mask]
```

Where	Means
internet-address-mask	Where subnet mask is defined using the same format as an Internet address, with ones for the network portion. The default is the natural mask fot the server's IP address.

Example

```
DEFINE SERVER IP SUBNET MASK 255.255.255.0
```

DEFINE/SET SERVER IP SUBNET MASK AUTOCONFIGURE Privilege: P

Use this command to allow the server to calculate a subnet mask automatically. Before you can set autoconfigure, you must disable the IP SUBNET MASK setting. See the DEFINE/SET SERVER IP SUBNET MASK command for more information.

In this case, the server selects a new value for the *internet-subnet-mask* based on the class of network (A, B, or C) of the current *internet-address*. When you allow the server to automatically determine the *internet-subnet-mask* (i.e., set the SERVER IP SUBNET MASK AUTOCONFIGURE characteristic to ENABLED), the server changes the *internet-subnet-mask* for either the permanent or operational database whenever the *internet-address* changes.

Use the INIT DELAY command to reboot the server in order for the changes to take effect.

SYNTAX

```
DEFINE SERVER IP SUBNET MASK AUTOCONFIGURE [ENABLED]
                                           [DISABLED]
```

Where	Means
AUTOCONFIGURE	If enabled, the software will use an *internet-subnet-mask* specified by the server manager, or one that has been determined automatically by the server.
ENABLED	The server will automatically determine the *internet-subnet-mask*.
DISABLED	The server will use an *internet-subnet-mask* specified by the server manager.

Example

```
Xyplex>> DEFINE SERVER IP SUBNET MASK AUTOCONFIGURE ENABLED
```

DEFINE/SET SERVER IP TCP CONNECT TIMER Privilege: P

Use this command to specify the number of seconds the server will wait for a response to a Telnet connect command before timing out.. Use the SHOW SERVER IP command to display the current timer value.

Syntax

```
XYPLEX> DEFINE/SET SERVER IP TCP CONNECT TIMER <number-of-seconds>
```

Where	Means
number-of-seconds	Specify how many seconds the server will wait for a response to a Telnet connect command before timing out. The valid values are 4 to 32 seconds. The default value is 32 seconds.

Example

```
XYPLEX> DEFINE SERVER IP TCP CONNECT TIMER 10
```

DEFINE SERVER IP TCP RESEQUENCING Privilege: P

Use this command to specify whether or not the server will store packets that it receives from a host that are out of sequence, or wait until the host resends the data.

Sometimes, when a host has a large amount of data to transmit to a server, the data will be divided among several smaller packets. Each packet is transmitted in sequence, with a sequence number. Occasionally, a packet will be delayed in transmission, usually by an intermediate destination. This can cause the packet to arrive out of sequence.

When a server receives packets out of sequence, it can either discard the data and not acknowledge receipt of the data, or it can collect the packets and wait until out-of-sequence packets are received before passing on the data in the proper sequence. When the server does not acknowledge the data, the host will retransmit all the information. When the server collects all the data until all the missing information is received, the server must expend additional memory in order to store all the collected data until the missing pieces are received. If the server has limited extra memory, it is recommended that you disable this command. If the server has sufficient memory to spare, or when host resources are a problem, you can enable TCP resequencing. If you do enable this setting, you may also need to increase the setting for the DEFINE/SET SERVER PACKET BUFFER characteristic.

Syntax

```
DEFINE SERVER IP TCP RESEQUENCING   [ENABLED]
                                    [DISABLED]
```

Where	Means
ENABLED	The server will attempt to resequence TCP/IP packets that it receives from the sender out of order, without waiting for the sender to retransmit.
DISABLED	The server will not acknowledge receipt of out-of-sequence packets, which will cause the sender to retransmit the packets. This is the default.

Example

```
Xyplex>> DEFINE SERVER IP TCP RESEQUENCING ENABLED
```

DEFINE/SET SERVER IP TCP RETRANSMIT Privilege: P

Use this command to set the initial TCP retransmit timeout value. This is the time when TCP will initially retransmit unacknowledged segments.

Syntax

```
DEFINE/SET SERVER IP TCP RETRANSMIT [time]
```

Where	Means
time	A value between 600 and 3000 milliseconds. The default is 640 milliseconds.

Example

```
DEFINE SERVER IP TCP RETRANSMIT 800
```

DEFINE/SET SERVER IP TRANSLATION TABLE TTL Privilege: P

Use this command to set the time-to-live for unreferenced translation table entries. Use the SHOW SERVER IP TRANLATION TABLE command to display the current value.

Syntax

```
DEFINE SERVER IP TRANSLATION TABLE TTL  <seconds>
```

Where	Means
seconds	Specify the time-to-live (in seconds) for unreferenced translation table entries. The valid values are 0 - 255 seconds. The default is 60 seconds.

Example

```
DEFINE SERVER IP TRANSLATION TABLE TTL 60
```

DEFINE/SET SERVER IP TTL Privilege: P

Use this command to specify the maximum amount of time that an Internet data packet can circulate through the network before the packet is discarded (i.e., "time to live"). When each packet is initially transmitted on the network, its time to live is equal to the *ttl-value* specified in the command. The current time to live for the packet is then decremented by 1 second, for each second that the packet is circulating through the network, or for each Internet gateway that the packet goes through.

Note that the SHOW SERVER IP CHARACTERISTICS display includes an "Internet TTL" field, which shows the current setting.

This command requires that the Telnet protocol is enabled.

Syntax

```
DEFINE/SET SERVER IP TTL ttl-value
```

Where	Means
ttl-value	The maximum amount of time, in seconds, that an Internet data packet can circulate through the network before the packet is discarded (i.e., "time to live"). Valid TTL-values are between 1 and 255 seconds (do not include the word "seconds" in the command). The default is 64 seconds.

Example

```
Xyplex>> DEFINE SERVER IP TTL 100
```

DEFINE/SET SERVER IPX FILTER DESTINATION NETWORK Privilege: P

Use this command to define filtering based on an IPX destination network.

See the Using TCP/IP Features section of the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE SERVER IPX FILTER DESTINATION NETWORK          [ipx-network]  [FORWARD]
                                                      [ALL]          [DISCARD]
```

Where	Means
ipx-network	The IPX network number of the destination network.
ALL	Filter on all destination networks.
FORWARD	Accept traffic to the specified destination. This is the default.
DISCARD	Refuse traffic to the specified destination.

Example

```
DEFINE SERVER IPX FILTER DESTINATION NETWORK ALL DISCARD
```

DEFINE/SET SERVER IPX FILTER DESTINATION NODE Privilege: P

Use this command to define filtering based on the node address of the destination IPX network.

See the Using the TCP/IP Filtering section of the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE/SET SERVER IPX FILTER DESTINATION NODE          [node-address][FORWARD]
                                                       [ALL]         [DISCARD]
```

Where	Means
node-address	The IPX address of the destination node.
ALL	Filter on all node addresses.
FORWARD	Accept all traffic to the destination node address specified. This is the default.
DISCARD	Refuse all traffic to the destination node address specified.

Example

```
DEFINE SERVER IPX FILTER DESTINATION NODE ALL DISCARD
```

DEFINE/SET SERVER IPX FILTER DESTINATION SOURCE Privilege: P

Use this command to define filtering based on destination and source criteria. See the Using the TCP/IP Features of the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE/SET SERVER IPX FILTER [destination-criteria][source-criteria]      [FORWARD]
                                                                          [DISCARD]
```

Where	Means

destination-criteria	Enter one of the following commands:
	`DESTINATION NETWORK [ipx-network]`
	`[ALL]`
	`DESTINATION NODE [node-address]`
	`[ALL]`

Where	Means
ipx-network	IPX network number of the destination network.
ALL	Filter on all IPX network/nodes.
node-address	The IPX node address of the destination node.

Where	Means

source-criteria	Enter one of the following commands:
	`SOURCE NETWORK [ipx-network]`
	`[ALL]`
	`SOURCE NODE [node-address]`
	`[ALL]`

Where	Means
ipx-network	IPX network number of the source network.
ALL	Filter on all IPX network/nodes.
node-address	The IPX node address of the source node.

FORWARD	Accept traffic to the destination(s) specified. This is the default.
DISCARD	Refuse traffic to the destination(s) specified.

Example

```
DEFINE SERVER IPX FILTER DESTINATION NODE ALL SOURCE NODE ALL DISCARD
```

DEFINE/SET SERVER IPX FILTER PACKET Privilege: P

Use this command to filter on a specific packet type or all packet types.

SYNTAX

```
DEFINE/SET SERVER IPX FILTER PACKET [hex-number]
                                    [ALL TYPE]
```

Where	Means
hex-number	Specify the hexadecimal number of the packet type.
ALL TYPE	All packet types will be filtered. This is the default.

DEFINE/SET SERVER IPX FILTER SOURCE NETWORK Privilege: P

Use this command to define filtering based on an IPX source network. See the Using TCP/IP Features in the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE/SET SERVER IPX FILTER SOURCE NETWORK  [ipx-network]     [FORWARD]
                                            [ALL]             [DISCARD]
```

Where	Means
ipx-network	The IPX network number of the source network.
ALL	Filter on all IPX networks.
FORWARD	Accept all traffic from the source network specified. This is the default.
DISCARD	Refuse traffic from the source network specified.

Example

```
DEFINE SERVER IPX FILTER SOURCE NETWORK ALL DISCARD
```

DEFINE/SET SERVER IPX FILTER SOURCE NODE Privilege: P

Use this command to define filtering based on the node address of the source IPX network. See the Using TCP/IP Features in the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE/SET SERVER IPX FILTER SOURCE NODE      [node-address]   [FORWARD]
                                              [ALL]            [DISCARD]
```

Where	Means
node-address	The IPX node address of the source node.
ALL	Filter on all IPX source node addresses.
FORWARD	Allow traffic to be received from the specified source node. This is the default.
DISCARD	Refuse traffic from the specified source node.

Example

```
DEFINE SERVER IPX FILTER SOURCE NODE ALL DISCARD
```

DEFINE SERVER IPX FILTERING Privilege: P

Use this command to enable or disable the IPX traffic filtering feature. By default, IPX traffic filtering is disabled. See the Using TCP/IP Features in the *Advanced Configuration Guide* for more information.

Use the INIT DELAY command to reboot the server in order for the change to take effect.

Syntax

```
DEFINE SERVER IPX FILTERING          [ENABLED]
                                     [DISABLED]
```

Where	Means
ENABLED	You can use IPX traffic filtering.
DISABLED	You cannot use IPX traffic filtering. This is the default setting.

Example

```
DEFINE SERVER IPX FILTERING ENABLED
```

DEFINE SERVER IPX INTERNAL NETWORK Privilege: P

Use this command to specify the "internal" IPX network number to use when transferring data between the Ethernet network and the PPP link(s).

The IPX protocol specification requires that IPX networks be identified by a network number. This permits efficient routing of packets to their destinations. Each device in a given IPX network must know its network number.

Access servers can obtain a network number in one of two ways:

- The server can "learn" its network number from other IPX devices (such as a Novell file server) that are connected to the same Ethernet network
- The server administrator can assign a network number

An access server uses a minimum of three unique network numbers. One network number is used for traffic that is sent or received on the Ethernet network. The second network number is used for traffic that is sent over a given PPP link, and a third network number is an "internal" network number, which is used inside the server for transferring information between the Ethernet network and the PPP link(s). The internal network number must not be used elsewhere in the Novell NetWare network (i.e., must be unique).

Syntax

```
DEFINE SERVER IPX INTERNAL NETWORK network-number
```

Where	Means
network-number	Specifies the internal IPX network number. Valid values for network-number are hexadecimal numbers between 1 (the default) and FFFFFFFE. The network number must not be used elsewhere in the Novell NetWare network.

Example

```
DEFINE SERVER IPX INTERNAL NETWORK 2
```

DEFINE SERVER IPX NETWORK Privilege: P

This command specifies the IPX network number to be used for communication between the server and devices on the Ethernet network, or to specify that the server should learn its network number from other IPX devices that is connected to the same Ethernet network.

The IPX protocol specification requires that IPX networks be identified by a network number. This permits efficient routing of packets to their destinations. Each device in a given IPX network must know its network number. Access servers can obtain a network number in one of two ways: the server can "learn" its network number from other IPX devices (such as a Novell file server) that are connected to the same Ethernet network, or the server administrator can assign a network number, using this command.

An access server uses a minimum of three unique network numbers. One network number is used for traffic that is sent or received on the Ethernet network. The second network number is used for traffic that is sent over a given PPP link, and a third network number is an "internal" network number, which is used inside the server for transferring information between the Ethernet network and the PPP link(s).

Syntax

```
DEFINE SERVER IPX NETWORK network-number
```

Where	Means
network-number	Specifies the IPX network number to be used for communication between the server and devices on the Ethernet network. Valid values are hexadecimal numbers between 0 (the default) and FFFFFFFE. When the network-number is set to 0, the server will learn its network number from other IPX devices on the Ethernet network to which it is connected. You would tend to specify a network-number when the server is connected to an Ethernet network that does not include other IPX devices (i.e., a "quiet" network). The default setting is 0.

Example

```
Xyplex>> DEFINE SERVER IPX NETWORK FFFFFFFE
```

DEFINE SERVER IPX PROTOCOL Privilege: P

This command specifies which type of IPX packet the server should use when communicating on the IPX network.

IPX is a protocol used by Novell NetWare. Xyplex access servers can accept four packet types over an IPX Interface: Ethernet-type packets, IEEE 802.2 (RAW), IEEE 802.3 (MAC), and IEEESNAP type packets. You can only use one of these types at a time. By default, Xyplex access servers are configured to use Ethernet-type packets for IPX. You must make sure that the protocol type you set for the server matches the value set at your Novell file server.

On a MAXserver 1450 or 1400A Printer Server, if you use the Setup Dialog, it will prompt you for this information, rather than require you to type in this command.

You must reboot the server using the INIT DELAY command, after making a change to the IPX packet type selection, in order for the change to take effect.

Syntax

```
DEFINE SERVER IPX PROTOCOL [ETHERNET]  [ENABLED]
                           [IEE802_2]  [DISABLED]
                           [MAC]
                           [IEESNAP]
```

Where	Means
ETHERNET	The access server will use Ethernet type packets when communicating on the network. This is the default.
IEE802_2	The access server will use IEE 802.2 (RAW) type packets when communicating.
MAC	The access server will use IEEE 802.3 (MAC) type packets when communicating.
IEESNAP	The access server will use IEE SNAP type packets when communicating.
ENABLED	Enables use of the specified packet type.
DISABLED	Disables use of the specified packet type.

Example

```
Xyplex>> DEFINE SERVER IPX PROTOCOL MAC ENABLED
```

DEFINE/SET SERVER IPX RIP BROADCAST Privilege: P

Use this command to specify whether or not the server will broadcast RIP information to other devices on the IPX network, and if the information is broadcast, how much information the server will send.

In some network configurations, an access server operates as an asynchronous IPX router. IPX routers exchange information about the networks to which they are attached, and the networks they can reach, via Router Information Protocol (RIP) packets. IPX routers use RIP information to route IPX packets. Each IPX router maintains a table of RIP information that it has received from other routers. IPX routers also broadcast RIP packets to neighboring routers periodically.

There are several commands available that control the broadcasting and storage of RIP information.

Syntax

```
DEFINE/SET SERVER IPX RIP BROADCAST    [FULL]
                                       [CHANGE]
                                       [NONE]
```

Where	Means
FULL	The server will broadcast the entire contents of the RIP table. The default is FULL.
CHANGE	The server will only broadcast new or changed routing information.
NONE	The server will not broadcast any routing information.

Example

```
Xyplex>> DEFINE SERVER IPX RIP BROADCAST FULL
```

DEFINE/SET SERVER IPX RIP BROADCAST DISCARD TIMEOUT Privilege: P

Use this command to specify how long the server keeps RIP information that it receives from other devices connected to the Ethernet network.

In some network configurations, an access server operates as an asynchronous IPX router. IPX routers exchange information about the networks to which they are attached, and the networks they can reach, via Router Information Protocol (RIP) packets. IPX routers use RIP information to route IPX packets. Each IPX router maintains a table of RIP information that it has received from other routers. IPX routers also broadcast RIP packets to neighboring routers periodically.

There are several commands available that control the broadcasting and storage of RIP information.

Syntax

```
DEFINE/SET SERVER IPX RIP BROADCAST DISCARD TIMEOUT timer-multiple
```

Where	Means
timer-multiple	How long the server keeps RIP information that it receives from other devices connected to the Ethernet network. The *timer-multiple* that you specify is multiplied by the value specified for the DEFINE/SET SERVER IPX RIP BROADCAST TIMER command. Valid values for *timer-multiple* are whole numbers between 0 and 4294967295. The default is 3.

Example

```
Xyplex>> DEFINE SERVER IPX RIP BROADCAST DISCARD TIMEOUT 5
```

DEFINE/SET SERVER IPX RIP BROADCAST TIMER Privilege: P

Use this command to specify how frequently the access server will broadcast RIP information on the Ethernet network.

In some network configurations, an access server operates as an asynchronous IPX router. IPX routers exchange information about the networks to which they are attached, and the networks they can reach, via Router Information Protocol (RIP) packets. IPX routers use RIP information to route IPX packets. Each IPX router maintains a table of RIP information that it has received from other routers. IPX routers also broadcast RIP packets to neighboring routers periodically.

There are several commands available that control the broadcasting and storage of RIP information.

Syntax

```
DEFINE/SET SERVER IPX RIP BROADCAST TIMER [timer-frequency]
```

Where	Means
TIMER-FREQUENCY	The frequency at which the access server will broadcast RIP information on the Ethernet network. Valid values are 0 and 4294967295 seconds. The default interval is 60 seconds.

Example

```
DEFINE SERVER IPX RIP BROADCAST TIMER 60
```

DEFINE/SET SERVER IPX RIP EXPORT Privilege: P

Use this command to define IPX RIP export filters. When you define the server it affects routes that the server learns through the attached LAN. When you define the Port, it affects routes that the server learns through a specified port.

See the DEFINE/SET PORT IPX RIP EXPORT command for port settings.

Syntax

```
DEFINE/SET  SERVER IPX RIP EXPORT NETWORK          [network][ADVERTISE]
                                                   [ALL]    [HIDE]
```

Where	Means
network	A hexadecimal value from 1 to FFFFFFFE.
ALL	Either restrict or accept all traffic.
ADVERTISE	Routes in the IPX route table will be advertised. This is the default.
HIDE	Routes in the IPX route table will be hidden.

Example

```
DEFINE SERVER IPX RIP EXPORT NETWORK ALL ADVERTISE
```

DEFINE SERVER IPX RIP IMPORT NETWORK Privilege: P

When IPX is enabled, the server adds all routes that it learns through RIP to its IPX route table. This process is called importing. Use this command to define filters that determine what the server does with its route table information.

Syntax

```
DEFINE SERVER IPX RIP IMPORT NETWORK [NETWORK]          [ACCEPT]
                                    [ALL]               [DISCARD]
```

Where	Means
network	A hexadecimal value from 1 to ffffffe.
ALL	All routes learned through RIP will be accepted or discarded (depending on the variable used in this command.
ACCEPT	The specified routes learned through RIP will be accepted. this is the default.
DISCARD	The specified routes learned through RIP will be discarded.

Example

```
DEFINE SERVER IPX RIP IMPORT NETWORK ALL ACCEPT
```

DEFINE SERVER IPX RIP MAXIMUM TABLE SIZE Privilege: P

Use this command to specify the maximum number of entries in the IPX Router Information Protocol (RIP) table.

Use the INIT DELAY command to reboot the server in order for the change to take effect.

In some network configurations, an access server operates as an asynchronous IPX router. IPX routers exchange information about the networks to which they are attached, and the networks they can reach, via Router Information Protocol (RIP) packets. IPX routers use RIP information to route IPX packets. Each IPX router maintains a table of RIP information that it has received from other routers. IPX routers also broadcast RIP packets to neighboring routers periodically.

There are several commands available that control the broadcasting and storage of RIP information.

Syntax

```
DEFINE SERVER IPX RIP MAXIMUM TABLE SIZE table-size
```

Where	Means
table-size	The maximum number of entries in the IPX Router Information Protocol (RIP) table. Valid values are 0 to 16000. If you specify 0, the server can maintain an unlimited number of entries. The default setting is 0.

Example

```
Xyplex>> DEFINE SERVER IPX RIP MAXIMUM TABLE SIZE 8000
```

DEFINE/SET SERVER IPX SAP BROADCAST Privilege: P

Use this command to specify whether or not the server will broadcast SAP information to other devices on the Ethernet network, and if the information is broadcast, how much information the server will send.

In some network configurations, an access server operates as an asynchronous IPX router. Servers in an IPX network (e.g., file servers, print servers) advertise their services through Service Advertising Protocol (SAP) packets. IPX servers also answer requests by clients who are looking for their services. IPX routers are responsible for broadcasting SAP information to other IPX routers in the network, and functioning as a proxy for servers on other networks. Each IPX router maintains a table of SAP information that it has received from neighboring routers and servers.

There are several commands available that control the broadcasting and storage of SAP information.

Syntax

```
DEFINE/SET SERVER IPX SAP BROADCAST     [FULL]
                                        [CHANGE]
                                        [NONE]
```

Where	Means
FULL	The server will broadcast the entire contents of the SAP table. This is the default.
CHANGE	The server will only broadcast new or changed routing information.
NONE	The server will not broadcast any routing information.

Example

```
Xyplex>> DEFINE SERVER IPX SAP BROADCAST CHANGE
```

DEFINE/SET SERVER IPX SAP BROADCAST DISCARD TIMEOUT Privilege: P

Use this command to specify how long the server keeps SAP information that it receives from other devices connected to the Ethernet network.

In some network configurations, an access server operates as an asynchronous IPX router. Servers in an IPX network (e.g., file servers, print servers) advertise their services through Service Advertising Protocol (SAP) packets. IPX servers also answer requests by clients who are looking for their services. IPX routers are responsible for broadcasting SAP information to other IPX routers in the network, and functioning as a proxy for servers on other networks. Each IPX router maintains a table of SAP information that it has received from neighboring routers and servers.

There are several commands available that control the broadcasting and storage of SAP information.

Syntax

```
DEFINE/SET SERVER IPX SAP BROADCAST DISCARD TIMEOUT timer-multiple
```

Where	Means
timer-multiple	How long the server keeps SAP information that it receives from other devices connected to the Ethernet network. The *timer-multiple* that you specify is multiplied by the value specified for the DEFINE/SET SERVER IPX SAP BROADCAST TIMER command. Valid values for *timer-multiple* are between 0 and 4294967295 seconds. The default is 3 seconds.

Example

```
DEFINE SERVER IPX SAP BROADCAST DISCARD TIMEOUT 5
```

DEFINE/SET SERVER IPX SAP BROADCAST TIMER Privilege: P

Use this command to specify how often the server will broadcast SAP information on the Ethernet network.

In some network configurations, an access server operates as an asynchronous IPX router. Servers in an IPX network (e.g., file servers, print servers) advertise their services through Service Advertising Protocol (SAP) packets. IPX servers also answer requests by clients who are looking for their services. IPX routers are responsible for broadcasting SAP information to other IPX routers in the network, and functioning as a proxy for servers on other networks. Each IPX router maintains a table of SAP information that it has received from neighboring routers and servers.

There are several commands available that control the broadcasting and storage of SAP information.

Syntax

```
DEFINE/SET SERVER IPX SAP BROADCAST TIMER timer
```

Where	Means
timer	Specifies how often the server will broadcast SAP information on the Ethernet network. Valid values are between 0 and 4294967295 seconds. The default interval is 60 seconds.

Example

```
DEFINE SERVER IPX SAP BROADCAST TIMER 60
```

DEFINE/SET SERVER IPX SAP EXPORT NETWORK Privilege: P

Use this command to define a server to advertise all Service Names and Types in its SAP table to other IPX routers, by default. This process is called exporting.

Syntax

```
DEFINE/SET SERVER IPX SAP EXPORT NETWORK [network]          [ADVERTISE]
                                        [ALL]              [Hide]
```

Where	Means
network	The network number of the server that will advertise all Service Names and Types to other IPX routers. It is a hexadecimal value from 1 to fffffffe.
ALL	All service names.
ADVERTISE	The service names and types will be advertised. This is the default.
HIDE	The service names and types will be hidden.

Example

```
DEFINE SERVER IPX SAP EXPORT NETWORK ALL ADVERTISE
```

DEFINE/SET SERVER IPX SAP EXPORT TYPE Privilege: P

Use this command to define the NetWare service type (print server, file server, etc.).

Syntax

```
DEFINE/SET SERVER IPX SAP EXPORT TYPE [type-value] [ADVERTISE]
                                      [ALL]        [HIDE]
```

Where	Means

type-value

type-value	**Description**
0	Unknown
1	User
2	User Group
3	Print Queue
4 or 278	File Server
5	Job Server
6	Gateway
7	Print Server
8	Archive Queue
9	Archive Server
A	Job Queue
B	Administration
24	Remote Bridge Server
47	Advertising Printer Server
107	Server (internal)

ALL	All service types. This is the default.
ADVERTISE	The specified service types will be advertised. This is the default.
HIDE	The specified service types will be hidden.

Example

```
DEFINE SERVER IPX SAP EXPORT TYPE ALL ADVERTISE
```

DEFINE/SET SERVER IPX SAP IMPORT NETWORK Privilege: P

Use this command to enable a server to add all service names and types that it learns through the SAP to its IPX SAP table.

Syntax

```
DEFINE/SET SERVER IPX SAP IMPORT NETWORK  [network]   [ACCEPT]
                                          [ALL]       [DISCARD]
```

Where	Means
network	A hexadecimal value from 1 to ffffffe.
ALL	All service names and types will be added to the server's IPX SAP table. This is the default.
ACCEPT	Accept all specified Service Names and Types. This is the default.
DISCARD	Discard all specified Service Names and Types.

Example

```
DEFINE SERVER IPX SAP IMPORT NETWORK ALL ACCEPT
```

DEFINE/SET SERVER IPX SAP IMPORT TYPE Privilege: P

Use this command to define the type of NetWare Services that will be added to the server's IPX SAP table.

Syntax

```
DEFINE/SET SERVER IPX SAP IMPORT TYPE  [type-value]   [ACCEPT]
                                       [ALL]          [DISCARD]
```

Where	Means

type-value

type-value	**Description**
0	Unknown
1	User
2	User Group
3	Print Queue
4 or 278	File Server
5	Job Server
6	Gateway
7	Print Server
8	Archive Queue
9	Archive Server
A	Job Queue
B	Administration
24	Remote Bridge Server
47	Advertising Printer Server
107	Server (internal)

ALL	All Service Names and Types. This is the default.
ACCEPT	Accept all specified Service Names and Types. This is the default.
DISCARD	Discard all Service Names and Types.

Example

```
DEFINE SERVER IPX SAP IMPORT TYPE ALL ACCEPT
```

DEFINE SERVER IPX SAP MAXIMUM TABLE SIZE Privilege: P

Use this command to specify the maximum number of entries in the IPX Service Advertisement Protocol (SAP) table.

Use the INIT DELAY command to reboot the server in order for this change to take effect.

In some network configurations, an access server operates as an asynchronous IPX router. Servers in an IPX network (e.g., file servers, print servers) advertise their services through Service Advertising Protocol (SAP) packets. IPX servers also answer requests by clients who are looking for their services. IPX routers are responsible for broadcasting SAP information to other IPX routers in the network, and functioning as a proxy for servers on other networks. Each IPX router maintains a table of SAP information that it has received from neighboring routers and servers.

There are several commands available that control the broadcasting and storage of SAP information.

Syntax

```
DEFINE SERVER IPX SAP MAXIMUM TABLE SIZE table-size
```

Where	Means
table-size	The maximum number of entries in the SAP table. Valid values are 0 to 16000 entries. If you specify 0, the server can maintain an unlimited number of entries. The default is 0.

Example

```
DEFINE SERVER IPX SAP MAXIMUM TABLE SIZE 8000
```

DEFINE/SET SERVER KEEPALIVE TIMER PRIVILEGE: P

Use this command to specify how long the server will transmit a null message over a LAT virtual circuit, when there is no other traffic originating at the server. The purpose of sending the null message is to notify circuit partner(s) that the server is still active.

As you increase the size of the timer-value, you will lengthen the time for other nodes to determine when the server goes down. However, as you decrease the size of this value, you increase the amount of network traffic.

The value you set for the KEEPALIVE TIMER also specifies how often the server will attempt to reconnect a session when there is a connection failure, for ports that have AUTOCONNECT set to ENABLED.

Note: *You cannot use the SET command to change this setting while there are active LAT sessions on the server.*

Syntax

```
DEFINE/SET SERVER KEEPALIVE TIMER timer-value
```

Where	Means
timer-value	How long the server will transmit a null message over a virtual circuit when there is no other traffic originating at the server, as well as how often the server will attempt to reconnect a session when there is a connection failure for ports that have AUTOCONNECT ENABLED. Valid values are between 10 and 180 seconds. The default value is 20 seconds.

Example

```
DEFINE SERVER KEEPALIVE TIMER 30
```

DEFINE SERVER KERBEROS Privilege: P

Use this command to enable or disable Kerberos Version 4 security features on the access server. No password is required to enable this feature.

If you are running Version 5.3.1 or later you can also use Kerberos Version 5. See the DEFINE SERVER KERBEROS FIVE command.

See the Security Features section of the *Advanced Configuration Guide* for more information.

After you enable the Kerberos security feature, use the INIT DELAY command to reboot the server for the changes to take effect.

Syntax

```
DEFINE SERVER KERBEROS  [ENABLED]
                        [DISABLED]
```

Where	Means
ENABLED	Enable Kerberos 4 on this server.
DISABLED	Disable Kerberos on this server. This is the default setting.

Example

```
Xyplex>> DEFINE SERVER KERBEROS ENABLED
```

DEFINE/SET SERVER KERBEROS ERROR MESSAGE Privilege: P

Use this command to specify the text in the Kerberos 739 error message. This error message appears if Kerberos authentication fails for any reason.

Syntax

```
DEFINE/SET SERVER KERBEROS ERROR MESSAGE "character string"
```

Where	Means
"*character-string*"	Text that appears in the Kerberos error message 739. The character string can be up to 132 ASCII characters and must be enclosed in double-quotes. The default string is "`Please contact your system administrator.`"

Example

```
DEFINE SERVER KERBEROS ERROR MESSAGE "Access denied. Please contact your
system administrator"
```

DEFINE SERVER KERBEROS FIVE Privilege: P

Servers running V5.3.1, or later, can be configured to authenticate users via either Kerberos version 4 or 5. (Prior to V5.3.1 only Kerberos version 4 is supported.) The Security Features section of the *Advanced Configuration Guide* describes how to configure a server to use Kerberos authentication. At the server, the Kerberos configuration procedure is the same for either version, except for the command change described below, and that SNMP must be also enabled on the server in order to use Kerberos version 5.

See the DEFINE/SET SERVER KERBEROS command to enable/disable Kerberos 4.

After you enable the Kerberos security feature, use the INIT DELAY command to reboot the server for the changes to take effect.

The SHOW/LIST/MONITOR SERVER KERBEROS display includes a "Kerberos version:" field that indicates which version of Kerberos is enabled on the unit.

Syntax

```
DEFINE SERVER KERBEROS FIVE   [ENABLED]
                              [DISABLED]
```

Where	Means
FIVE	Specifies that Kerberos version 5 should be enabled or disabled. If you do not include the keyword "FIVE" in the command, the server will enable or disable Kerberos version 4 authentication.
ENABLED	Enable the Kerberos version 5.
DISABLED	Disable the Kerberos version 5. This is the default.

Example

```
Xyplex>> DEFINE SERVER KERBEROS FIVE ENABLED
```

DEFINE/SET SERVER KERBEROS MASTER Privilege: P

Use this command to specify the *domain-name* or *internet-address* of the Kerberos Master. The Kerberos Master maintains the Kerberos databaseand provides information to primary or secondary Server hosts within a realm. A primary or secondary server must query the Master when a user changes a Kerberos password.

See the Security Features section of the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE/SET SERVER KERBEROS MASTER   [domain-name]
                                    [internet-address]
                                    [NONE]
```

Where	Means
domain-name	The Domain name of the Kerberos Master host.
internet-address	The Internet address of the Kerberos Master host.
NONE	Remove the Kerberos Master host, and use NONE as the domain-name. This is the default.

Example

```
DEFINE SERVER KERBEROS MASTER 140.179.224.100
```

DEFINE/SET SERVER KERBEROS PASSWORD PORT Privilege: P

Use this command to specify the port number of the password change service on the Kerberos master.

Syntax

```
DEFINE/SET SERVER KERBEROS PASSWORD PORT [port number]
```

Where	Means
port number	A decimal number between 1 and 32767. The default *number* is 749.

Example

```
DEFINE SERVER KERBEROS PASSWORD PORT 760
```

DEFINE/SET SERVER KERBEROS PASSWORD SERVICE Privilege: P

Use this command to specify the name of the Kerberos password change service on the Kerberos master.

Syntax

```
DEFINE/SET SERVER KERBEROS PASSWORD SERVICE [service-name]
```

Where	Means
service-name	The name of the password change service with a maximum length of 16 characters. The default *character-string* is “kadmin.”.

Example

```
Xyplex>> DEFINE SERVER KERBEROS PASSWORD SERVICE AaBbCc
```

DEFINE/SET SERVER KERBEROS PORT Privilege: P

Use this command to specify the Kerberos port number that the server uses in connections to the Kerberos server.

Syntax

```
DEFINE/SET SERVER KERBEROS PORT [number]
```

Where	Means
number	A decimal number of either 88 or 750. The default *number* is 750.

Example

```
DEFINE SERVER KERBEROS PORT 88
```

DEFINE/SET SERVER KERBEROS PRIMARY/SECONDARY SERVER Priv: P

Use these commands to specify the *domain-name* or *internet-address* of the Kerberos primary or secondary Server host. The primary Server host is the first Server host to be queried for user verification. The server queries the secondary Server host if the primary Server host does not respond.

See the Security Features section of the *Advanced Configuration Guide* for more information

Syntax

```
DEFINE/SET SERVER KERBEROS [PRIMARY] SERVER  [domain-name]
                           [SECONDARY]       [internet-address]
                                             [NONE]
```

Where	Means
domain-name	Specifies the Domain name of the Kerberos primary or secondary Server host.
internet-address	Specifies the Internet address of the Kerberos primary or secondary Server host.
NONE	Remove the Kerberos primary or secondary server, and use NONE as the domain-name. This is the default.

Example

```
DEFINE SERVER KERBEROS PRIMARY SERVER 140.179.224.100
```

DEFINE/SET SERVER KERBEROS QUERY LIMIT Privilege: P

Enables you to specify the maximum number of Server host queries the server can make when attempting to verify a Kerberos ID. When this limit is reached, the server logs out the port and generates an error message. The limit also specifies the maximum number of Master queries the server can make when attempting to change a user's password.

Syntax

```
DEFINE/SET SERVER KERBEROS QUERY LIMIT limit
```

Where	Means
limit	The maximum number of queries the server can make when attempting to verify a Kerberos ID or change a password. Valid values are 1 through 16. The default query limit is 3.

Example

```
DEFINE SERVER KERBEROS QUERY LIMIT 5
```

DEFINE/SET SERVER KERBEROS REALM Privilege: P

Use this command to specify the name of the Kerberos realm to which the primary and secondary Server hosts are associated.

Syntax

```
DEFINE/SET SERVER KERBEROS REALM ["realm-name"]
                                 [NONE]
```

Where	Means
"*realm-name*"	The name of the Kerberos realm to which the Master and Server hosts are associated. The realm name can be up to 40 characters and must be enclosed in quotes. Use the following format for a Kerberos name: username.instance@realm. Note: The Realm name is case sensitive.
NONE	A Kerberos Realm does not exist for this server. Use this keyword to eliminate a previously defined Kerberos realm name. This is the default setting.

Example

```
DEFINE SERVER KERBVEROS REALM MEDICAL-NETWORK
```

DEFINE/SET SERVER KERBEROS SECURITY Privilege: P

Use this command to specify whether the server is to provide Kerberos user verification.

Syntax

```
DEFINE/SET SERVER KERBEROS SECURITY [LOGIN]
                                   [NONE]
```

Where	Means
LOGIN	The server will provide Kerberos user verification.
NONE	The server will not provide Kerberos user verification. This is the default.

Example

```
DEFINE SERVER KERBEROS SECURITY LOGIN
```

DEFINE/SET SERVER LAT IMMEDIATE ACK Privilege: P

Use this command to control whether the access server acknowledges a LAT message immediately or waits until the circuit timer expires.

Syntax

```
DEFINE/SET SERVER LAT IMMEDIATE ACK [ENABLED]
                                    [DISABLED]
```

Where	Means
ENABLED	The access server acknowledges a LAT message immediately.
DISABLED	The access server waits until the circuit timer expires.

Example

```
DEFINE SERVER LAT IMMEDIATE ACK ENABLED
```

DEFINE/SET SERVER LAT SOLICITS Privilege: P

This command allows you to specify whether or not a server will issue LAT multicast service requests when a user requests connection to an unknown service. LAT servers and hosts normally advertise the services which they make available to other servers by means of LAT announcements.

The server will store information locally about these services, so that when a user requests a service, the server knows where to locate that service. When the server does not know the location of a service, it can be configured to issue a LAT multicast message on the network, requesting a service announcement from any devices on the network at which the requested service is available. This is called a LAT solicit.

Typically, you will not need to enable LAT solicits, since the server will store information about all available services. If, however, you have restricted the number of services or nodes that the server is permitted to store information about, it may be possible for the server to be missing information about an available service (See Server Default Settings in the *Configuration Guide* for more information). In this case, you might want to enable LAT solicits. Enabling LAT solicits can result in many LAT multicast messages being issued on the network by the server.

Syntax

```
DEFINE/SET SERVER LAT SOLICITS      [ENABLED]
                                    [DISABLED]
```

Where	Means
ENABLED	The server will issue LAT multicast service requests, when a user requests connection to an unknown service.
DISABLED	The server will not issue LAT multicast service requests, when a user requests connection to an unknown service.

Example

```
DEFINE SERVER LAT SOLICITS ENABLED
```

DEFINE SERVER LOAD IP ADDRESS Privileged: P

This command specifies the IP address for DTFTP loading.

Use this command if DTFTP is enabled for the software image loading. You must also specify the IP address of the load host and the name of the file that contains the load image. If the access server gains access to the load host through a gateway, you must also specify the IP address of the gateway. Use the DEFINE SERVER LOAD IP commands to specify this information.

The Internet address of the access server appears in the SHOW SERVER IP display. When you define the address for DTFTP loading, it appears in the LIST SERVER LOADDUMP CHARACTERISTICS display.

Syntax

DEFINE SERVER LOAD [*record*/ALL] IP ADDRESS *internet-address*

Where	Means
[record]	One or more of the following initialization records: PRIMARY SECONDARY TERTIARY ALL The PRIMARY initialization record is the default.
internet-address	The Internet load address of the access server.

Example

```
DEFINE SERVER LOAD IP ADDRESS 150.169.70.133
```

DEFINE/SET SERVER LOAD IP DELIMITER Privilege: P

Use this command to specify the file delimiter that the host should use during a DTFTP load. Use the LIST SERVER LOADDUMP CHARACTERISTICS command to display the current value.

Use this command if DTFTP is enabled for the software load image. You must also specify the Internet address of the load host and the name of the file that contains the load image. If the access server gains access to the load host through a gateway, you must also specify the Internet address of the gateway. Use the DEFINE SERVER LOAD IP commands to specify this information.

The Internet address you specify with this command overrides the IP address you specify with the DEFINE/SET SERVER IP ADDRESS command if they are different, until the server has completed the boot-up process.

Syntax

```
DEFINE SERVER LOAD IP DELIMITER [“message-string”]
```

Where	Means
message-string	Specify the file delimiter such as "\" or "/" that the host should use during a DTFTP parameter loading.

Example

```
DEFINE SERVER LOAD IP DELIMITER "/"
```

DEFINE SERVER LOAD IP LOAD FILE Privilege: P

This command specifies the path and name of the file that contains the software load image on the Internet host you specify for DTFTP loading.

Use this command if DTFTP is enabled for the software image loading. You must also specify the Internet address of the access server. If the access server gains access to the load host through a gateway, you must also specify the Internet address of the gateway. Use the other DEFINE SERVER LOAD IP commands to specify this information.

When you define the Internet load file for DTFTP loading, it appears in the LIST SERVER LOADDUMP CHARACTERISTICS display.

Syntax

```
DEFINE SERVER LOAD [record] IP FILE "/pathname/filename"
```

Where	Means
[record]	Specifies one or more of the following initialization records: PRIMARY SECONDARY TERTIARY ALL The PRIMARY initialization record is the default.
"/pathname/filename"	The path and filename of the file that contains the software load image. Most UNIX implementations are case-sensitive, so be sure to use the appropriate upper- and lower-case letters in the filename, or the host may not recognize it. Enclose the pathname and filename in quotes. If just a filename is specified without a path, then the default "/tftpboot/" will be used.

Example

```
DEFINE SERVER LOAD IP FILE "/usr2/xpcsrv20.sys"
```

DEFINE SERVER LOAD IP GATEWAY Privilege: P

This command specifies the IP address of a gateway router on the network for DTFTP software image loading. Only access servers that use a gateway router to gain access to an IP load host through DTFTP require that you specify a gateway address with this command.

Use this command if DTFTP is enabled for the software load image. You must also specify the IP address of the load host and the name of the file that contains the load image. If the access server gains access to the load host through a gateway, you must also specify the IP address of the gateway. Use the DEFINE SERVER LOAD IP commands to specify this information.

When you define the IP gateway address for DTFTP loading, it appears on the LIST SERVER LOADDUMP CHARACTERISTICS display.

Syntax

```
DEFINE SERVER LOAD   [record] IP GATEWAY [internet-address]
```

Where	Means
record	Specify one or more of the following initialization records: PRIMARY SECONDARY TERTIARY ALL The PRIMARY initialization record is the default.
internet-address	The IP address of the gateway.

Example

```
DEFINE SERVER LOAD INTERNET GATEWAY 150.122.30.164
```

DEFINE SERVER LOAD IP LOAD HOST Privilege: P

This command specifies the IP address of the host where the software load image resides.

Use this command if DTFTP is enabled for the software image loading. You must also specify the Internet address of the load host and the name of the file that contains the load image. If the access server gains access to the load host through a gateway, you must also specify the Internet address of the gateway. Use the DEFINE SERVER LOAD IP commands to specify this information.

When you define the IP address of the load host for DTFTP loading, it appears on the SERVER LOADDUMP CHARACTERISTICS display.

Syntax

```
DEFINE SERVER LOAD [record] IP HOST [internet-address]
```

Where	Means
record	One or more of the following initialization records: PRIMARY SECONDARY TERTIARY ALL The PRIMARY initialization record is the default.
internet-address	The Internet address of the host that contains the software load image.

Example

This example specifies an internet address for the load host that contains the software load image.

```
DEFINE SERVER LOAD IP HOST 150.122.30.155
```

DEFINE SERVER LOAD PROTOCOL Privilege: P

Use this command to specify one or all load protocols to use when the access server searches for a software load image file or a parameter file. You specify whether the protocol applies to the software load image or the parameter file in the command line.

By default, a MAXserver attempts to obtain the software load image using the CARD protocol and the parameter file using the NVS protocol. If a card is not present, or the NVS protocol is disabled, the access server attempts to obtain these files using other protocols in this order: DTFTP, XMOP, MOP, BOOTP, RARP. All of these protocols except DTFTP are enabled by default. If you use the keyword ALL to enable all protocols, you also enable DTFTP.

You cannot use DTFTP to load the parameter file except on the Network 9000 Access Server 720 which doesn't have NVS. If you do enable DTFTP, specify the following IP addresses:

- The load host
- The access server
- The gateway router to the load host, if necessary

Use the DEFINE SERVER LOAD IP commands to specify this information.

Syntax

```
DEFINE SERVER LOAD [record] [usage] PROTOCOL [protocol-name] [ENABLED]
                                                              [DISABLED]
```

Where	Means
[record]	Use one or more of the following initialization records: PRIMARY SECONDARY TERTIARY ALL The PRIMARY initialization record is the default.
usage	Use one of the following keywords, which indicate whether you are specifying a protocol for a software load image or a parameter file: IMAGE PARAMETERS

DEFINE SERVER LOAD PROTOCOL (continued)

protocol Specify one of the following keywords which represent different protocols:

Protocol	Means
NVS	NonVolatile Storage protocol for the parameter file
CARD	Local memory card protocol for the load image
XMOP	Xyplex MOP Protocol
MOP	Digital Equipment Corporation Maintenance Operations Protocol
BOOTP	Bootstrap protocol
RARP	UNIX Reverse Address Resolution Protocol
DTFTP	UNIX Directed Trivial File Transfer Protocol (software load image only)
ALL	All protocols (you cannot disable all load protocols)

For loading parameters on older MAXserver units use either NVS or remote protocols, but not both types.

Note: Xyplex Access Servers cannot load from a DEC Info Server or any other device that does not support loading via DEC MOP V3 using all 5 parameters (Including the fifth parameter, which is the Host date/time stamp) for "Parameter Load with Transfer Address" using MOP.

ENABLED Enable the protocol in the initialization records you specify. You can enable only one protocol in the command line, unless you use the keyword ALL to enable all protocols.

DISABLED Disable the protocol in the initialization records you specify. You cannot use the keyword ALL to disable all load protocols.

Examples

```
DEFINE SERVER LOAD PRIMARY IMAGE PROTOCOL DTFTP ENABLED

DEFINE SERVER LOAD SECONDARY PARAMETERS PROTOCOL RARP DISABLED
```

DEFINE SERVER LOAD SOFTWARE Privilege: P

This command specifies the CARD/XMOP/MOP filename for the software load image.

You specify this filename if CARD, XMOP, or MOP is enabled as a load protocol for the software image, and the image name is different than the default. The default CARD/MOP/XMOP software image filename is XPCSRV20 for MAXserver 1604/1608A/1608B/1620/1640 and Network 9000 Access Server 720.

Use the LIST SERVER LOADDUMP CHARACTERISTICS screen to display the load image filename.

Syntax

```
DEFINE SERVER LOAD [record] SOFTWARE [filename]
```

Where	Means
record	Use one or more of the following initialization records: PRIMARY SECONDARY TERTIARY ALL The PRIMARY initialization record is the default. **Note:** Older access server units (e.g., MX1600, MX1450) have only one INIT record, so this keyword is not specified.
filename	A CARD/XMOP/MOP filename, which can consist of up to 16 characters. Note: Xyplex Access Servers cannot load from a DEC Info Server or any other device that does not support loading via DEC MOP V3 using all 5 parameters (Including the fifth parameter, which is the Host date/time stamp) for "Parameter Load with Transfer Address" using MOP.

Example

```
DEFINE SERVER LOAD SECONDARY SOFTWARE XPCSRV20

DEFINE SERVER LOAD SOFTWARE XPCS00S
```

DEFINE SERVER LOADDUMP Privilege: P

Use this command to disable or enable an initialization record. MAXserver 1604/1608A/1608B/1620 and 1640 access servers have only the primary initialization record enabled by default. You must enable the other initialization records if you want the access server to use them.

All initialization records have default values for the loading and dumping protocols, and the CARD/XMOP/MOP load image filename, whether they are enabled or disabled by default.

You cannot disable all three initialization records. If the primary and secondary initialization records are disabled, for example, you cannot disable the tertiary initialization record. If you attempt to do so, the server generates an error message.

See the *Getting Started with MAXserver Access Servers* guide for more information.

Syntax

```
DEFINE SERVER LOADDUMP  [record] [DISABLED]
                                 [ENABLED]
```

Where	Means
[record]	Use one or more of the following initialization records: PRIMARY SECONDARY TERTIARY ALL The PRIMARY initialization record is the default.
ENABLED	Enable the initialization records you specify. Only the primary record is enabled by default.
DISABLED	Disable the initialization records you specify. You cannot disable all three initialization records.

Examples

```
DEFINE SERVER LOADDUMP SECONDARY ENABLED
```

```
DEFINE SERVER LOADDUMP ALL ENABLED
```

DEFINE SERVER LOADDUMP DEFAULT Privilege: P

Use this command to reset the parameters in one or more initialization records to the factory default settings. Initialization parameters include the status of the initialization record, protocols, the CARD/XMOP/MOP load image filename, and the Internet characteristics for DTFTP loading. You can change this information through the ROM Initialization Configuration Menu and through SNMP

The default settings for the primary initialization record on an access server are as follows:

Parameter	Default Settings
Status	ENABLED
Load Image Protocols	CARD, XMOP, MOP, BOOTP, RARP
Dump Protocols	XMOP, MOP, BOOTP, RARP
Parameter Protocols	NVS, XMOP, MOP, BOOTP, RARP
Software filename	XPCSRV20

The secondary and tertiary initialization records on the MAXserver 1604/1608/1620 and 1640 are disabled by default. If you reset one of these initialization records to its default settings the the initialization record will be disabled. See the DEFINE SERVER LOADDUMP command for information about how to enable and disable initialization records.

Note: Xyplex Access Servers cannot load from a DEC Info Server or any other device that does not support loading via DEC MOP V3 using all 5 parameters (Including the fifth parameter, which is the Host date/time stamp) for "Parameter Load with Transfer Address" using MOP.Syntax

```
DEFINE SERVER LOADDUMP [record] DEFAULT
```

Where	Means
[record]	Use one or more of the following initialization records: PRIMARY (default) SECONDARY TERTIARY ALL

Example

```
DEFINE SERVER LOADDUMP SECONDARY DEFAULT
```

DEFINE SERVER LOAD STATUS MESSAGE Privilege: P

Use this command to enable or disable the loading of status messages.

You might want to disable this feature during the software loading process if a device such as a bar code reader, which cannot interpret status messages, is connected to a serial port.

Use the LIST SERVER LOADDUMP CHARACTERISTICS command to display the current status of the status message.

Syntax

```
DEFINE SERVER LOAD STATUS MESSAGE [ENABLED]
                                  [DISABLED]
```

Where	Means
ENABLED	Status messages display during the loading process. This is the default.
DISABLED	Status messages will not display during the loading process.

Example

```
DEFINE SERVER LOAD STATUS MESSAGE DISABLED
```

DEFINE/SET SERVER LOCK Privilege: P

Use this command to specify whether or not users with interactive terminals can lock their ports (use the LOCK command) to prohibit unauthorized use of their terminals while they are absent.

Syntax

```
DEFINE/SET SERVER LOCK  [DISABLED]
                        [ENABLED]
```

Where	Means
DISABLED	Users cannot use the LOCK command to prohibit use of their terminals while they are absent.
ENABLED	Users can use the LOCK command to prohibit use of their terminals while they are absent. This is the default setting.

Example

```
DEFINE SERVER LOCK DISABLED
```

DEFINE/SET SERVER LOGIN PASSWORD Privilege: P

Use this command to specify the password that interactive users must type when they log on to a server port for which the PORT PASSWORD characteristic is set to ENABLED. If you type the password on the DEFINE/SET SERVER LOGIN PASSWORD command line, enclose the password in quotation mark characters ("). If you do not type the password on the DEFINE/SET SERVER LOGIN PASSWORD command line, the system will prompt you for a password. In this case, do not enclose the password in quotation mark characters. You can disable the login password on port 0. However, certain programs, such as TSM, Scriptor, and ControlPoint, require a password. These programs will not function properly if you disable the password on port 0.

Syntax

```
DEFINE/SET SERVER LOGIN PASSWORD "password"
```

Where	Means
"password"	The new password that interactive users must type when they log on to a server port. The password can from 1 - 16 characters. The default password is "ACCESS". There is only one login password per server.

Example

```
DEFINE SERVER LOGIN PASSWORD "ACCESS"
```

DEFINE/SET SERVER LOGIN PROMPT Privilege: P

Use this command to specify that you will define or change the prompt that is displayed to users to request that they type the login password.

Syntax

```
DEFINE/SET SERVER LOGIN PROMPT "prompt-string"
```

Where	Means
"prompt-string"	The prompt that is displayed to users to request the login password. The prompt can be from 1 to 8 characters. Enclose the prompt text in quotation marks ("). During login, the server will include an ASCII bell character (i.e., the server will cause the terminal to "beep") with the login prompt. The default prompt is "#."

Example

```
DEFINE SERVER LOGIN PROMPT "PASSWORD"
```

DEFINE/SET SERVER LPD QUEUE Privilege: P

Use this command to enable or disable LPD queues. You must enable an LPD queue at the server in order for the server to be able to accept LPD print jobs from hosts. The LPD queue name at the server must correspond to a remote printer name in the LPD configuration at a host. There can be multiple LPD queues on a server. Multiple ports can also be assigned to service an LPD queue. In this case, a print job submitted to the LPD queue will be serviced by the first available port.

When an LPD queue is enabled, it will accept print jobs from any appropriately configured host. When an LPD queue is disabled, it will reject further print jobs, but will continue to process jobs that are currently in the queue. The host is free to try to resubmit the job at a later time. (To completely eliminate a queue and all jobs in it, use the CLEAR LPD QUEUE command. To remove a specific job from an LPD queue, use the lprm or REMOVE QUEUE ENTRY command. These commands will not work after the job has started.)

Define the LPD print queue settings in the following order to successful process print job in the queue:

1. Define the queue name and enable (the queue name must correspond to a remote printer name).

2. Specify which ports will support LPD queues.

3. Specify whether the server will convert line-feed characters in to carriage returns (LFCR).

4. Specify whether or not the server will use formfeed between each print job (FF).

See the *Printer Configuration Guide* for more information on the LPD daemon. See the *Using the Xyplex ULI* Guide for a description of the lpc, lpq, and lprm commands that are available at the access server.

The LPD daemon must be enabled in order to enable an LPD queue. The ULI must be enabled in order to use the LPC, LPQ, and LPRM commands at the server.

Syntax

```
DEFINE/SET SERVER LPD QUEUE   ["queue-name"]    [ENABLED]
                              [ALL]             [DISABLED]

DEFINE/SET SERVER LPD QUEUE ["queue-name"] PORT [port-list]
                            [ALL]

DEFINE/SET SERVER LPD QUEUE ["queue-name"] FF [ENABLED]
                                              [DISABLED]
```

DEFINE/SET SERVER LPD QUEUE (continued)

```
DEFINE/SET SERVER LPD QUEUE ["queue-name"] LFCR [ENABLED]
                                                [DISABLED]
```

Where	Means
"*queue-name*"	The name of the LPD queue. The queue name must match the name of a remote printer that you specify at a UNIX host (for example, in the /etc/printcap file or to the AT&T UNIX lpadmin utility). The name can be up to 16 characters long, and is case sensitive. Enclose the name in double-quotation marks ("). You can specify ALL for all queues.
PORT	The LPD queue will exist at one or more ports, other than the current port.
port-list	One or more access server ports where LPD queue will exist.
ENABLED	The LPD queue will be enabled at the port(s).
DISABLED	The LPD queue will be disabled at the port(s). When you disable an LPD queue, the server will not accept additional print jobs directed to that LPD queue. The server will process print jobs which are currently in the LPD queue.
LFCR	Specify whether or not the server will convert line-feed characters into carriage-return/line-feed characters.
ENABLED	The server will convert line-feed characters into carriage-return/line-feed characters. Typically, you would set the LFCR characteristic to ENABLED for line printers or printers which are intended to process simple documents. When the LFCR characteristic is ENABLED, the port will imitate the operation of a printer that is directly connected to a UNIX host.
DISABLED	The server will not convert line-feed characters into carriage-return/line-feed characters. Typically, you would use set the LFCR characteristic to DISABLED for laser printers, PostScript printers, etc.
FF	Specify whether or not the server will formfeed after, before or NONE between each print job.

Examples

```
DEFINE SERVER LPD QUEUE "line-printer" ENABLED

DEFINE SERVER LPD QUEUE "line-printer" PORT 1-2

DEFINE SERVER LPD QUEUE "laser-printer" FF ENABLED

DEFINE SERVER LPD QUEUE ALL LFCR DISABLED
```

DEFINE/SET SERVER LPD QUEUE BYPASS Privilege: P

Use this command to define whether or not a port on a LPD queue should be bypassed when the port is in a XOFF'd condition (such as when the printer is out of paper)..

***Note**: Use this command only with queues that have more than one port defined to them.*

Syntax

```
DEFINE SERVER LPD QUEUE <queue-name> BYPASS ENABLED
```

Where	Means
queue-name	The name of the LPD queue that will be bypassed.
ENABLED	The LPD port will be bypassed when it is in XOFF'd condition. All subsequent print jobs will be sent to the next LPD port. The LPD port must be configured with the same queue name. You should only bypass LPD ports that have other ports configured with the same queue name and are operational.
DISABLED	The port will not be bypassed when it is in an XOFF'd condition.

Example

```
DEFINE LPD QUEUE 1234 BYPASS ENABLED
```

DEFINE/SET SERVER MAINTENANCE PASSWORD Privilege: P

Use this command to change the password that users must type when they want to use certain commands at the server, such as the REMOTE CONSOLE command and the DECnet NCP TRIGGER or NCP LOAD commands. If you type the password on the DEFINE/SET SERVER MAINTENANCE PASSWORD command line, enclose the password in quotation mark characters ("). If you do not type the password on the DEFINE/SET SERVER MAINTENANCE PASSWORD command line, the system will prompt you for a password. In this case, do not enclose the password in quotation mark characters. Refer to the description of the REMOTE CONSOLE command for an example of maintenance password use.

Syntax

`DEFINE/SET SERVER MAINTENANCE PASSWORD` *`password`*

Where	Means
password	The new password that users must type in order to use the REMOTE CONSOLE command and the DECnet NCP TRIGGER and NCP LOAD commands at this server. The password is a hexadecimal number in the range of 0 to FFFFFFFFFFFFFFFF (i.e., up to 16 hexadecimal digits long). The default password is 0. You can disable the MAINTENANCE PASSWORD characteristic by specifying the default password. There can be only one maintenance password per server.

Example

```
Xyplex>> DEFINE SERVER MAINTENANCE PASSWORD "FAE7"
```

DEFINE SERVER MENU Privilege: P

Use this command to specify whether or not a system manager can develop a menu with up to 20 selections for the server, or to add new items to the menu.

See the section on Menus in the *Advanced Configuration Guide* for more information.

You must reboot the server using the INIT DELAY command before you can define individual menu items.

Syntax

```
DEFINE SERVER MENU     [ENABLED]
                       [DISABLED]
                       [item-number  "string1"]
```

After you press the RETURN key, you are prompted to enter a Xyplex command with the prompt:

Enter Xyplex command> *string2*

Where	Means
ENABLED	Designated ports at this server can be configured to use the menu interface.
DISABLED	Designated ports at this server cannot be configured to use the menu interface. This is the default.
item-number	The item number (1 - 20) on the server's menu that you want to add or modify.
string1	A string enclosed in quotes (") containing the text of the menu item to be included. (30 characters maximum).
string2	The Xyplex command string to be executed when the menu item defined in *string1* is selected. The string can contain multiple commands separated by semicolons (64 characters maximum).

Example

```
DEFINE SERVER MENU ENABLED

DEFINE SER MENU 1 "Telnet to UNIX Host A."

Enter XYPLEX command > telnet 140.179.241.10
```

DEFINE/SET SERVER MENU CONTINUE PROMPT Privilege: P

Use this command to specify the text that prompts the user to press the keyboard RETURN key in order to continue a menu operation, at ports for which the menu is enabled.

Syntax

```
DEFINE/SET SERVER MENU CONTINUE PROMPT [“prompt-text”]
```

Where	Means
"prompt-text"	Display this text as the user prompt to press the keyboard RETURN key in order to continue a menu operation at ports where this menu feature is enabled. The text string can be up to 50 characters. Enclose the string in quotation marks ("). The default text string is "press <RETURN> to continue."

Example

```
Xyplex>> DEFINE SERVER MENU PROMPT "press RETURN to continue."
```

DEFINE/SET SERVER MENU PROMPT Privilege: P

Use this command to change the text that prompts the user to select a menu entry from the Server Menu.

Syntax

```
DEFINE/SET SERVER MENU PROMPT "prompt-text"
```

Where	Means
"prompt-text"	Display this text when a user selects a menu entry from the Server Menu. The text string can be up to 50 characters. Enclose the string in quotation marks ("). The default text string is "Enter number of selection or use arrow keys:."

Example

```
DEFINE SERVER MENU PROMPT "Select a menu number."
```

DEFINE/SET SERVER MULTICAST TIMER Privilege: P

Use this command to specify how often the server will issue an announcement to notify service nodes and other servers of the availability of LAT services. This setting only applies when ANNOUNCEMENTS is ENABLED, and when there are local LAT services defined (i.e., announcements are not made if there are no local services defined).

When you change the multicast timer value, you manage the relationship (or trade-off) between the amount of network traffic and the frequency at which nodes obtain information about locally available services.

Syntax

```
DEFINE/SET SERVER MULTICAST TIMER timer-value
```

Where	Means
timer-value	Specifies the time interval at which the server transmits a LAT service announcement. Valid values are from 10 to 180 seconds (do not supply units). The default value is 30 seconds.

Example

```
Xyplex>> DEFINE SERVER MULTICAST TIMER 20
```

DEFINE SERVER MULTISESSIONS Privilege: P

Use this command to specify whether or not ports on this unit will support DEC terminals, such as the VT330 and VT420 models, which provide a feature called Dual Session Management. This feature enables users to display and control multiple simultaneous communication sessions. The sessions can be multiplexed (i.e., combined) onto a single serial line to a host

You must reboot the server using the INIT DELAY command before this setting is operational.

Syntax

```
DEFINE SERVER MULTISESSIONS          [ENABLED]
                                     [DISABLED]
```

Where	Means
ENABLED	Ports on this server will support terminals that use Dual Session Management.
DISABLED	Ports on this server will not support terminals which use Dual Session Management. This is the default

Example

```
DEFINE SERVER MULTISESSIONS ENABLED

Multisession Password> xxxxxxx (password will not be displayed)
```

NOTE: *Contact your Xyplex Sales Representative if you do not have a password. This features does not support VT5xx terminal multisessions.*

DEFINE/SET SERVER NAME Privilege: P

Use this command to specify a unique name for the server. This name will be used to identify the server for CONNECT commands made at other servers and for host-initiated connections.

Syntax

```
DEFINE/SET SERVER NAME server-name
```

Where	Means
server-name	A unique server name. The server name can be between 1 and 16 characters. **Do not** enclose the server-name in quotation marks. The server will convert all lowercase letters to uppercase letters. The default server-name is a seven-character name in the form Xnnnnnn, where nnnnnn represents the last 6 digits of the server Ethernet address. For servers that operate with a parameter server that is a VAX/VMS node, the default name is the DECnet node name that has been assigned by the system manager of that node.

Example

```
DEFINE SERVER NAME X01FE87
```

DEFINE SERVER NESTED MENU NAME Privilege: P

Use this command to specify the name of the menu file on the script server. When the access server initializes with memory allocated for a menu file, it searches the script server for the filename you specify.

The filename displays in the Menu Name field on the SHOW/LIST/MONITOR SERVER CHARACTERISTICS screen.

Syntax

```
DEFINE SERVER NESTED MENU NAME "string"
```

Where	Means
"*string*"	The name of the menu file on the script server. It can be from 1 to 16 characters. Enclose the string in quotes.

Example

```
Xyplex>> define server nested menu name "n.menu.file"
```

DEFINE SERVER NESTED MENU SIZE Privilege: P

Use this command to specify how much access server memory you want to reserve for nested menus. Allocating memory with this command also enables the Nested Menu feature. Allocating 0 bytes disables the feature.

If you allocate memory for nested menus, and then do not use all of it, you can release the unused memory. Use this command and specify only the amount of memory that the menus require. When you initialize the access server after you reallocate the memory, the access server frees up the unused memory.

You must reboot the server using the INIT DELAY command for this setting to take effect.

The Nested Menu Size field in the SHOW/LIST/MONITOR SERVER CHARACTERISTICS display shows the total amount of memory, in bytes, that you have allocated for nested menus. The Nested Menu Memory field of the SHOW/LIST/MONITOR SERVER STATUS display shows the current amount of memory, in bytes, being used by the menu file.

See the Nested Menus section in the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE SERVER NESTED MENU menu-size
```

Where	Means
menu-size	The amount of memory, in bytes, that you want to reserve for nested menus. Valid entries are from 0 through 204,800. Entering 0 disables the nested menu feature and deallocates any previously allocated memory for this feature. The default is 0 bytes (Nested Menus disabled).

Example

```
DEFINE SERVER NESTED MENU SIZE 150000
```

DEFINE/SET SERVER NODE LIMIT Privilege: P

Use this command to specify the maximum number of LAT service nodes about which the server will maintain information.

You should be careful to limit this value, as the number of nodes that the server maintains information about affects other server resources which rely on the server's memory pool. See the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE/SET SERVER NODE LIMIT  [limit]
                              [NONE]
```

Where	Means
limit	The maximum number of service nodes about which the server will maintain information. Valid values are 1 to 1000. The default value is 100.
NONE	The server will maintain information about as many service nodes as memory permits.

Example

```
DEFINE SERVER NODE LIMIT NONE
```

DEFINE/SET SERVER NUMBER Privilege: P

Use this command to specify a number by which the server may be identified from other servers. The number you specify is for informational purposes only.

Syntax

```
DEFINE/SET SERVER NUMBER server-number
```

Where	Means
server-number	Specifies the number which will be assigned to the server to distinguish it from other servers. Valid values are from 0 to 32767. The default value is 0.

Example

```
DEFINE SERVER NUMBER 355
```

DEFINE SERVER OVERRIDE INTERNAL ADDRESS Privilege: P

Use this command to permit or inhibit the access server from overriding the defined IP address with that obtained from the ROMs via the loading protocol.

Syntax

```
DEFINE SERVER OVERRIDE INTERNAL ADDRESS   [ENABLED]
                                          [DISABLED]
```

Where	Means
ENABLED	The server will override the defined IP address with that obtained from ROM. This is the default.
DISABLED	The server will not override the defined IP address with that obtained from ROM.

Example

```
DEFINE SERVER OVERRIDE INTERNAL ADDRESS ENABLED
```

DEFINE SERVER PACKET COUNT Privilege: P

At initialization time, the server sets aside memory for storing packets of data that are waiting to be passed on to another internal server process, both for incoming and outgoing data. Use this command to control the maximum number of incoming and outgoing packets used by internal server processes that can be buffered in server memory. Using this feature lets you increase the server's ability to handle large amounts of incoming data at the expense of reducing the amount of memory that is available for other features. For example, you might increase the number of available packet buffers if the server is configured to have many serial ports continuously receiving or outputting data at high speeds (19,200 bps or greater).

Notes: *If the packet buffers are increased to the point where there is only between 0 and 160K of memory, a message displays that states the recommended amount of memory has been exceeded, but you will still be able to use the new value.*

If the packet buffer is increased to the point that there is not enough installed memory for the requested value, a message displays stating that the unit needs more memory and the define will NOT be done.

Use the SHOW SERVER CHARACTERISTICS command to display the current packet count setting. You should only consider increasing the setting if the "Packet Buffers" field on the SERVER ALTERNATE STATUS display indicates that there have been failures. The server allocates 1556 bytes of memory for each additional packet buffer.

Reboot the server using the INIT DELAY command for this setting to take effect.. You should only consider increasing the setting for the SERVER PACKET COUNT characteristic if the "Packet Buffers" field on the S;.

Syntax

```
DEFINE SERVER PACKET COUNT [packet-buffers]
```

Where	Means
packet-buffers	The maximum number of incoming and outgoing packets. For load images that require at least 2MB of memory to run, valid values are 80 to 4088. For load images that can be used with less memory, valid values are 80 to 160. The default value is 80. This command is memory managed. If the memory needed exceeds the value that has been defined, the proper error messages will be displayed.

Example

```
DEFINE SERVER PACKET COUNT 200
```

DEFINE/SET SERVER PARAMETER SERVER CHECK Privilege: P

Use this command to change the following parameter server settings:

- How the server locates or updates eligible parameter servers
- Whether or not the server will attempt to locate additional eligible parameter servers
- Whether or not the server can use TFTP or Xyplex proprietary protocols for parameter serving
- How often the server will check the parameter servers to save changes made since the last check.

When this feature is enabled, the server will try to locate all specified parameter servers at the specified intervals and save parameter changes made since the last check.

Syntax

```
DEFINE/SET SERVER PARAMETER SERVER CHECK      [DISABLED]
                                              [ENABLED]*
                                              [PROPRIETARY ENABLED]
                                              [TFTP ENABLED]
                                              [timer-value]
```

Where	Means
DISABLED	The server does not attempt to locate additional eligible parameter servers.
ENABLED	The server attempts to locate eligible parameter servers. This is the default setting.
PROPRIETARY ENABLED	The server uses a Xyplex proprietary protocol to locate eligible parameter servers. To use only the proprietary protocol for this purpose, disable all parameter server checking (use the DEFINE SERVER PARAMETER SERVER CHECK DISABLED command), then enable checking using proprietary protocol (use the DEFINE SERVER PARAMETER SERVER CHECK PROPRIETARY ENABLED command).
TFTP ENABLED	Specifies that the server uses TFTP to locate eligible parameter servers. To use only TFTP for this purpose, disable all parameter server checking (use the DEFINE SERVER PARAMETER SERVER CHECK DISABLED command), then enable checking using TFTP (use the DEFINE SERVER PARAMETER SERVER CHECK TFTP ENABLED command).
timer-value	Specifies the time interval at which the server attempts to locate eligible parameter servers. Valid values are between 1 to 120. The default is 30 minutes.

Example

```
DEFINE SERVER PARAMETER SERVER CHECK TFTP ENABLED

DEFINE SERVER PARAMETER SERVER CHECK 120
```

DEFINE/SET SERVER PARAMETER SERVER PATH Privilege: P

Use this command to specify the complete directory pathname to be used when writing parameter files.

Some TFTP implementations require that a unit supply a complete directory name (a "path") when that unit tries to use TFTP to write a file. This requirement can affect Xyplex units when they attempt to store parameter files at UNIX hosts. By defining the complete pathname you can specify exactly where parameter files will be stored.

Syntax

```
DEFINE/SET SERVER PARAMETER SERVER PATH "directory-path"
```

Where	Means
"*directory-path*"	The name of the directory where parameter files can be located. A valid *directory-path* can be a string up to 40 characters long, ending with a forwards slash character (/). Enclose the *directory-path* in quotation marks (").

Example

```
Xyplex>> DEFINE SERVER PARAMETER SERVER PATH "/tftpboot/"
```

DEFINE/SET SERVER PARAMETER SERVER LIMIT Privilege: P

Use this command to specify the maximum number of eligible parameter servers for which this server will retain information.

Syntax

```
DEFINE/SET SERVER PARAMETER SERVER LIMIT number
```

Where	Means
number	Valid values are from 1 to 8 parameter servers. The default is 4.

Example

```
Xyplex>> DEFINE SERVER PARAMETER SERVER LIMIT 5
```

DEFINE/SET SERVER PARAMETER SERVER RETRANSMIT Privilege: P

Use this command to change the number of attempts the server will make to update parameter information at a parameter server which does not acknowledge the attempt, and the frequency at which the server will update parameter information at a parameter server which has not acknowledged an update attempt.

Syntax

```
DEFINE/SET SERVER PARAMETER SERVER RETRANSMIT  [LIMIT limit]
                                               [TIMER timer-value]
```

Where	Means
LIMIT	Specifies that you will change the number of attempts the server will make to update parameter information at a parameter server which does not acknowledge the attempt.
limit	The number of attempts the server will make to update parameter information at a parameter server that does not acknowledge the attempt. Valid values are 1 through 100. The default is 3.
TIMER	Specifies that you will change the frequency at which the server will update parameter information at a parameter server which has not acknowledged an update attempt.
timer-value	The time interval at which the server attempts to update parameter information at a parameter server which has not acknowledged an update attempt. Valid values are between 1 and 30 minutes (do not specify units). The default is 5 minutes.

Example

```
DEFINE SERVER PARAMETER SERVER RETRANSMIT LIMIT 5

DEFINE SERVER PARAMETER SERVER RETRANSMIT TIMER 3
```

DEFINE/SET SERVER PASSWORD LIMIT Privilege: P

Use this command to specify the maximum number of times which the server will prompt the user to enter the correct privileged password or login before the server logs out the port.

Syntax

```
DEFINE/SET SERVER PASSWORD LIMIT          [limit]
                                          [NONE]
```

Where	Means
limit	How many times the server will prompt the user to enter the correct privileged password. When the limit is reached, the server logs out the port. Valid values are 0 through 250. The default value is 3.
NONE	The server will prompt the maximum number of times (250) for the user to enter the correct privileged password, before the server logs out the port.

Example

```
DEFINE SERVER PASSWORD LIMIT 3
```

DEFINE/SET SERVER PAP REMOTE PASSWORD Privilege: P

Use this command to specify the password that the server will send to a remote device which requires a password in order to establish a PPP connection.

A remote device can be configured to require that the port (the local end of a PPP connection) provides a password prior to establishing a PPP connection and forwarding data. Although it is possible to configure a link so that a password is required in either direction, both directions, or no direction, the DEFINE/SET SERVER PAP REMOTE PASSWORD command only applies when the remote device requires a password. There is only one PPP PAP remote password for the server. If a remote device requires a password, and none has been specified, the server will send a "blank" password and the connection will not be formed.

Note that the Xyplex PPP implementation does not require that PAP authentication be used in both directions to establish a PPP connection. The Xyplex PPP implementation can be configured to require that remote devices must supply the login password in order to establish a PPP connection with the port. Refer to the DEFINE/SET PORT PAP ENABLED/DISABLED command description.

When the remote device requires a password, the server will send its nodename and the password specified by the DEFINE/SET SERVER PAP REMOTE PASSWORD command.

Syntax

```
DEFINE/SET SERVER PAP REMOTE PASSWORD "password"
```

Where	Means
"password"	The password that the server will send to a remote device which requires a PAP password in order to establish a PPP connection. The password can consist of up to 16 characters. Enclose the *password* in double quotation marks ("). To disable a previously enabled password, use a null string enclosed in double quotation marks (i.e., "").

Example

```
DEFINE SERVER PAP REMOTE PASSWORD "gumby"
```

DEFINE SERVER PPP CHAP REMOTE PASSWORD Privilege: P

Use this command to configure the authentication password used by the server when authenticating itself to a peer using CHAP. The password is viewable and can be a string of characters.

Syntax

```
DEFINE/SET SERVER PPP CHAP REMOTE PASSWORD "quoted-string"
```

Where	Means
"*quoted -string*"	The password that the server will send to a remote device which requires a CHAP password in order to establish a PPP connection. The password can consist of up to 16 characters. Enclose the *password* in double quotation marks ("). To disable a previously enabled password, use a null string enclosed in double quotation marks (i.e., "").

Example

```
DEFINE SERVER PPP CHAP REMOTE PASSWORD "AaBbCc"
```

DEFINE/SET SERVER PRIVILEGED PASSWORD Privilege: P

Use this command to specify the password that users must type when they want to use privileged server commands. If you type the password on the DEFINE/SET SERVER PRIVILEGED PASSWORD command line, enclose the password in quotation marks ("). If you do not type the password on the command line, the system will prompt you for a password. In this case, do not enclose the password in quotation mark characters.

IMPORTANT

If the default password SYSTEM is changed with this command, make sure that the new password is written down in a safe location. If you forget the password, the server will need to be reset to factory default settings.

Syntax

```
DEFINE/SET SERVER PRIVILEGED PASSWORD "password"
```

Where	Means
"password"	The new password that users must type in order to use privileged server commands. The password can be between 1 and 16 characters. The default password is SYSTEM. There can be only one privileged password per server.

Example

```
Xyplex>> DEFINE SERVER PRIVILEGED PASSWORD "MANANGER"
```

DEFINE SERVER PROTOCOL ARAP Privilege: P

Use this command to specify whether or not ARAP can be used on a given server. Please note that this is a keyed feature. Contact your Xyplex Sales Representative to purchase this feature.

The AppleTalk Remote Access Protocol (ARAP) allows a Macintosh user to connect to an AppleTalk network through a Xyplex server. The server transfers AppleTalk packets between the remote Macintosh and the AppleTalk network in such a way that the Macintosh acts as though it were directly connected to the network. See the *Basic Configuration* Guide for more information.

You must reinitialize the server using the INIT DELAY command before the changes will take effect.

Syntax

```
DEFINE SERVER PROTOCOL ARAP   [ENABLED]
                              [DISABLED]
```

Where	Means
ENABLED	The ARAP feature can be used on this server.
DISABLED	The ARAP feature cannot be used on this server. This is the factory default.

Example

```
DEFINE SERVER PROTOCOL ARAP ENABLED
```

The server will respond with the following prompt:

```
ARAP Password>
```

Enter the protocol password at this password prompt. The server will not "echo" the protocol password to the display. Press the <RETURN> key. When you supply the correct password, the following messages appear:

```
Press <RETURN> to modify configuration, any other key to abort.
```

DEFINE SERVER PROTOCOL IPX Privilege: P

Use this command to enable or disable the IPX protocol on the access server. As of Version 6.0.4, a password is no longer needed to enable this feature on image "xpcsrv20.sys" for the following units: MAXserver 1604/1608/1620/1640 and Network 9000 720 access servers.

When IPX is disabled, the memory used by IPX becomes available for use by the access server. You cannot disable the IPX protocol if the TELNET protocol is disabled. Reboot the server using the INIT DELAY command in order for the change to take effect.

Syntax

```
DEFINE SERVER PROTOCOL IPX    [ENABLED]
                              [DISABLED]
```

Where	Means
ENABLED	Enable the IPX protocol on the access server.
DISABLED	Disable the IPX protocol on the access server.

Examples

```
DEFINE SERVER PROTOCOL IPX DISABLED
```

DEFINE SERVER PROTOCOL LAT Privilege: P

Use this command to enable or disable the LAT protocol on the access server. When LAT is disabled, the memory used by LAT becomes available for use by the access server. The LAT protocol cannot be disabled if the TELNET protocol is disabled.

On a MAXserver 1100/1120 unit, if you specify only one protocol (LAT or TELNET) in a DEFINE SERVER PROTOCOL command, the server will enable that protocol and disable the other, without requiring a password. A Xyplex-supplied password is required to enable LAT and TELNET simultaneously on a MAXserver 1100/1120 unit. Contact Xyplex Customer Support if you do not have a password. LAT is enabled by default for all other unit types and no password is needed to enable/disable LAT.

Reboot the server using the INIT DELAY command in order for the change to take effect.

Syntax

```
DEFINE SERVER PROTOCOL LAT          [ENABLED]
                                    [DISABLED]
```

Where	Means
ENABLED	Enable the LAT protocol on the access server. This is the factory default setting for this protocol on all units except the MAXserver 1100/1120.
DISABLED	Disable the LAT protocol on the access server.

Examples

```
DEFINE SERVER PROTOCOL LAT DISABLED
```

To enable LAT and Telnet at the same time, issue the following command:

```
DEFINE SERVER PROTOCOL LAT ENABLED TELNET ENABLED
```

See also DEFINE SERVER PROTOCOL MX800.

DEFINE SERVER PROTOCOL MX800 Privilege: P

Use this command to allow a MX800 Access Server with more than 1MB of RAM installed to load the xpcs00s.sys image (supported through Software Version 6.0.2). This command only applies to the MX800, and is not supported in the current software.

Syntax

```
DEFINE SERVER PROTOCOL MX800  [ENABLED]
                              [DISABLED]
```

Where	Means
ENABLED	Load the xpcs00s.sys image from a remote host.
DISABLED	Cannot load the image from a remote host.

DEFINE SERVER PROTOCOL PPP Privilege: P

Use this command to enable or disable the PPP protocol on the access server. When PPP is disabled, the memory used by PPP becomes available for use by the access server.

PPP does not require a software password. PPP runs only on units that support a Multi-Megabyte load image.

Reboot the server using the INIT DELAY command in order for the change to take effect.

Syntax

```
DEFINE SERVER PROTOCOL PPP          [ENABLED]
                                    [DISABLED]
```

Where	Means
ENABLED	Enable the PPP protocol.
DISABLED	Disable PPP protocol. This is the default.

Example

```
DEFINE SERVER PROTOCOL PPP ENABLED
```

DEFINE SERVER PROTOCOL SNMP Privilege: P

Use this command to enable or disable the SNMP protocol on the access server. When SNMP is disabled, the memory used by SNMP becomes available for use by the access server.

No password is needed to enable or disable SNMP.

Reboot the server using the INIT DELAY command in order for the change to take effect.

Syntax

```
DEFINE SERVER PROTOCOL SNMP      [ENABLED]
                                 [DISABLED]
```

Where	Means
ENABLED	Enable the SNMP protocol on the access server. This is the default.
DISABLED	Disable SNMP protocol on the access server.

Examples

```
Xyplex>> DEFINE SERVER PROTOCOL SNMP DISABLED
```

DEFINE SERVER PROTOCOL TELNET Privilege: P

Use this command to enable or disable the TELNET protocol on the access server. You cannot disable TELNET if the LAT protocol is disabled. The TELNET protocol must be enabled in order for the TN3270 protocol to be enabled.

On a MAXserver 1100/1120 unit, if you specify only one protocol (LAT or TELNET) in a DEFINE SERVER PROTOCOL command, the server will enable that protocol and disable the other, without requiring a password. A Xyplex-supplied password is required to enable LAT and TELNET simultaneously on a MAXserver 1100/1120 unit. Contact Xyplex Customer Support if you do not have a password. TELNET is enabled by default for all other unit types and no password is needed to enable/disable TELNET.

Reboot the server using the INIT DELAY command in order for the change to take effect.

Syntax

```
DEFINE SERVER PROTOCOL TELNET       [ENABLED]
                                    [DISABLED]
```

Where	Means
ENABLED	Enable the TELNET protocol on the access server. This is the factory default setting for this protocol on all units except the MAXserver 1100/1120.
DISABLED	Disable the TELNET protocol on the access server.

Examples

```
DEFINE SERVER PROTOCOL TELNET DISABLED
```

To enable LAT and TELNET at the same time, issue the following command:

```
DEFINE SERVER PROTOCOL LAT ENABLED TELNET ENABLED
```

See also SERVER PROTOCOL MX800.

DEFINE SERVER PROTOCOL TN3270 Privilege: P

Use this command to enable or disable the TN3270 protocol on the access server.

See the TN3270 section of the *Advanced Configuration Guide* for more information about configuring the access server to support TN3270.

You cannot disable the TELNET protocol if the LAT protocol is disabled. The TELNET protocol must be enabled in order for the TN3270 protocol to be enabled.

When TN3270 is disabled, the memory used by TN3270 becomes available for use by the access server.

Reboot the server using the INIT DELAY command in order for the change to take effect.

TN3270 is a keyed feature and requires a software password. Contact your Xyplex sales representative if you do not have a password.

Syntax

```
DEFINE SERVER PROTOCOL TN3270    [ENABLED]
                                 [DISABLED]
```

Where	Means
ENABLED	Enable the TN3270 protocol on the access server.
DISABLED	Disable the TN3270 protocol on the access server. This is the factory default.

Examples

```
DEFINE SERVER PROTOCOL TN3270 DISABLED
```

DEFINE SERVER PROTOCOL XPRINTER Privilege: P

Use this command to enable or disable the XPRINTER protocol on the access server. Units with at least 2 megabytes of memory can support this protocol. As of Version 6.0.4 software a password is no longer needed to enable this feature on image "xpcsrv20.sys" for the following units: MAXserver 1604/1608/1620/1640 and Network 9000 720.

You must reboot the server using the INIT DELAY command before the changes can take effect.

See the *Printer Configuration Guide* for more information.

Syntax

```
DEFINE SERVER PROTOCOL XPRINTER  [ENABLED]
                                 [DISABLED]
```

Where	Means
ENABLED	Enable the XPRINTER protocol on the access server.
DISABLED	Disable XPRINTER protocol on the access server. This is the default setting.

Example

```
DEFINE SERVER PROTOCOL XPRINTER ENABLED
```

DEFINE SERVER PROTOCOL XREMOTE Privilege: P

Use this command to enable or disable the Xremote protocol on the access server. Units with at least 2 megabytes of memory can support this protocol. As of Version 6.0.4, a password is no longer needed to enable this feature on image "xpcsrv20.sys" for the following units: MAXserver 1604/1608/1620/1640 and Network 9000 720 access servers.

You must reboot the server using the INIT DELAY command before the changes can take effect.

See the XREMOTE section of the *Basic Configuration Guide* for more information.

Syntax

```
DEFINE SERVER PROTOCOL XREMOTE   [ENABLED]
                                 [DISABLED]
```

Where	Means
ENABLED	Enable the Xremote protocol on the access server.
DISABLED	Disable Xremote protocol on the access server. This is the default setting.

Example

```
DEFINE SERVER PROTOCOL XREMOTE ENABLED
```

DEFINE/SET SERVER PURGE GROUP Privilege: P

Use this command to specify whether or not the server should remove LAT reachable nodes from the node database, whenever you change the setting(s) for the PORT AUTHORIZED GROUPS or the SERVER SERVICE GROUPS. The reachable nodes that are removed are those associated with LAT service groups that are no longer available for the server or port.

Syntax

```
DEFINE/SET SERVER PURGE GROUP       [DISABLED]
                                    [ENABLED]
```

Where	Means
DISABLED	The server should not remove LAT reachable nodes from the node database whenever you change the PORT AUTHORIZED GROUPS or SERVER SERVICE GROUPS setting(s). This is the default.
ENABLED	The server should remove LAT reachable nodes from the node database whenever you change the PORT AUTHORIZED GROUPS or SERVER SERVICE GROUPS setting(s).

Example

```
Xyplex>> DEFINE SERVER PURGE GROUP ENABLED
```

DEFINE/SET SERVER PURGE NODE Privilege: P

Use this command to specify whether or not the server should remove LAT reachable nodes from the node database, whenever the limit specified by the SERVER NODE LIMIT setting is reached.

Syntax

```
DEFINE/SET SERVER PURGE NODE        [DISABLED]
                                    [ENABLED]
```

Where	Means
DISABLED	The server should not remove LAT reachable nodes from the node database, whenever the limit specified by the SERVER NODE LIMIT is reached. This is the default.
ENABLED	The server should remove LAT reachable nodes from the node database whenever the limit specified by the SERVER NODE LIMIT is reached.

Example

```
DEFINE SERVER PURGE NODE ENABLED
```

DEFINE/SET SERVER QUEUE LIMIT Privilege: P

Use this command to specify the maximum number of unsatisfied connection requests that can be in the connection queue (i.e., requests made for connection to a service which is busy).

Syntax

```
DEFINE/SET SERVER QUEUE LIMIT       [queue-limit]
                                    [NONE]
```

Where	Means
queue-limit	The maximum number of unsatisfied connection requests in the connection queue. Valid values are from 0 to 100. The default value is 24 connections. To disable the connection request queue, specify 0.
NONE	The server connection queue can contain as many unsatisfied connection requests as memory permits.

Example

```
DEFINE SERVER QUEUE LIMIT 0
```

DEFINE SERVER RADIUS Privilege: P

Use this command to enable or disable the Radius authentication feature on your access server. See the Security Features section of the *Advanced Configuration Guide* for more information about how to configure the server to support Radius.

You must reboot the server using the INIT DELAY command before the change takes effect.

Syntax

```
DEFINE SERVER RADIUS    [ENABLED]
                        [DISABLED]
```

Where	Means
ENABLED	Enables the Radius feature.
DISABLED	Disables the Radius feature. This is the default setting.

Example

```
DEFINE SERVER RADIUS ENABLED
```

DEFINE/SET SERVER RADIUS ACCOUNTING Privilege: P

Use this command to specify the number of the port that will use Radius Accounting, and to define how many times the access server will attempt to log the accounting record of both the primary and secondary servers before giving up and failing.

See the Using Security Features section of the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE/SET SERVER RADIUS ACCOUNTING [PORT] [port number]

                                    [ATTEMPTS] [number-of-attempts]
```

Where	Means
PORT	The UDP port for account logging. The default is 1646.
port number	The port that will use Radius Accounting
ATTEMPTS	You are specifying that the server should attempt to access the account record
number-of-attempts	The number of times the server should attempt to access the accounting record for both the primary and secondary servers before giving up and failing. The default setting is 5.

Example

```
DEFINE SERVER RADIUS ACCOUNTING ATTEMPTS 5
```

DEFINE/SET SERVER RADIUS CHAP CHALLENGE SIZE Privilege: P

Use this command to define the size of the CHAP Challenge sent to a PPP peer for CHAP and to the RADIUS server for verification.

Note: *The current Radius servers only support challenge sizes of 16 characters.*

Syntax

```
DEFINE/SET SERVER RADIUS CHAP CHALLENGE SIZE [challenge-size]
```

Where	Means
challenge-size	Currently, the only challenge size supported is 16 characters.

Example

```
DEFINE SERVER RADIUS CHAP CHALLENGE SIZE 16
```

DEFINE/SET SERVER RADIUS LOGGING Privilege: P

Use this command to enable or disable Radius client packet logging. This command saves Radius status information or debug information.

See the Security Features Section of the *Advanced Configuration Guide* for more information about configuring the server to support Radius.

Syntax

```
DEFINE/SET SERVER RADIUS LOGGING    [ENABLED]
                                    [DISABLED]
```

Where	Means
ENABLED	Enables Radius-specific logging information.
DISABLED	Disables Radius-specific logging information. This is the default.

Example

```
DEFINE SERVER RADIUS LOGGING ENABLED
```

DEFINE/SET SERVER RADIUS PORT Privilege: P

Use this command to specify the UDP port that the Radius client and server use for communication.

Syntax

DEFINE/SET SERVER RADIUS PORT *port number*

Where	Means
port number	The port number over which to communicate with the Radius server. Valid values are from 1 to 65535. The default value is 1645

Example

```
Xyplex>> DEFINE SERVER RADIUS PORT 1645
```

DEFINE/SET SERVER RADIUS PRIMARY/SECONDARY SECRET Privilege: P

Use this command to specify the primary and secondary Radius secret shared between the Radius client and the Radius server used for encryption communications between them. The secret is separately configurable for each server.

Syntax

```
DEFINE/SET SERVER RADIUS [PRIMARY]   SECRET "secret"
                         [SECONDARY]
```

Where	Means
PRIMARY	The primary Radius server host.
SECONDARY	The secondary Radius server host.
SECRET	Shared secret with Radius server.
"secret"	A text string, enclosed in double quotes, of up to 32 characters. The string is case-sensitive. The default value is "Default_Secret"

Example

```
DEFINE SERVER RADIUS PRIMARY SECRET "AaBbCc"
```

DEFINE/SET SERVER RADIUS PRIMARY/SECONDARY SERVER Privilege: P

Use this command to specify the primary and secondary Radius database servers and their associated address or hostname. The secondary server is used only after the communication with the primary server fails. The secondary server is not used as a second attempt when a user authentication fails.

Syntax

```
DEFINE/SET SERVER RADIUS [PRIMARY} SERVER [ip-address]
                         [SECONDARY]      [domain-name]
                                          [NONE]
```

Where	Means
PRIMARY	Primary Radius host.
SECONDARY	Secondary Radius host.
ip_address	IP address of the Radius server host.
domain-name	Internet domain name of the Radius server host.
NONE	There is no server assigned as either the primary (if primary is specified) or secondary (if secondary is specified) server.

Example

```
DEFINE SERVER RADIUS PRIMARY SERVER radhost.xyplex.com

DEFINE SERVER RADIUS SECONDARY SERVER NONE
```

DEFINE/SET SERVER RADIUS SERVER RETRY Privilege: P

Use this command to configure the number of retries to the Radius server for both Radius Authentication and Radius Accounting.

Syntax

```
DEFINE/SET SERVER RADIUS SERVER RETRY [number-of-retries]
```

Where	Means
number-of-retries	The number of retries to the Radius server. The default value is 3, and the valid range is 1 through 10.

Example

```
DEFINE SERVER RADIUS SERVER RETRY 6
```

DEFINE/SET SERVER RADIUS TIMEOUT Privilege: P

Use this command to configure the time to wait for a Radius server to respond before retransmitting packets to the server.

Syntax

```
DEFINE/SET SERVER RADIUS TIMEOUT [time}
```

Where	Means
time	The time between Radius client retransmissions to the server when trying to authenticate a user. The default is 5 seconds.

Example

```
DEFINE SERVER RADIUS TIMEOUT 5
```

DEFINE/SET SERVER RELIABLE ACCOUNTING Privilege: P

Use this command to specify whether the server accepts a registration request for accounting data. A host on the network must be configured to register with the Xyplex server and accept the reliable accounting session via TCP.

Syntax

```
DEFINE/SET SERVER RELIABLE ACCOUNTING  [ENABLED]
                                       [DISABLED]
```

Where	Means
ENABLED	The server can accept a registration request for accounting data, and upon registration send accounting data using a reliable TCP session pipe to the host that initiated the registration request.
DISABLED	The server cannot accept a registration request for accounting data. This is the default setting.

Example

```
DEFINE SERVER RELIABLE ACCOUNTING ENABLED
```

See Also

```
DEFINE/SET SERVER ACCOUNTING ENTRIES
DEFINE/SET SERVER VERBOSE ACCOUNTING
DEFINE/SET SERVER VERBOSE ACCOUNTING PRIORITY
```

DEFINE/SET SERVER REPORT ERRORS Privilege: P

Use this command to specify whether or not the server will display error messages when invalid or unsupported commands are issued by a user or a TSM script.

This command also controls the display of error messages for the following SET/DEFINE SERVER commands that are not supported by TCP/IP-LAT software: CONSOLE and HEARTBEAT. It also controls the reporting of error messages when a user attempts to issue a command that is not supported by the parallel port of a network printer server or a modem-control-related command for a port that does not support modem signals.

It also controls the display of error messages for the following DEFINE/SET PORT commands that are not supported by TCP/IP-LAT software: ALTERNATE SPEED, RING, INPUT SPEED, and OUTPUT SPEED.

Syntax

```
DEFINE/SET SERVER REPORT ERRORS      [ENABLED]
                                     [DISABLED]
```

Where	Means
ENABLED	The server will display error messages when an invalid or unsupported command is issued. When the REPORT ERRORS setting is enabled, the invalid command is ignored but error messages are reported. The "ENABLED Characteristics" field on the SERVER CHARACTERISTICS display will list Report Errors when this feature has been enabled.
DISABLED	The server will not display error messages when an invalid or unsupported command is issued. When the REPORT ERRORS setting is DISABLED, the invalid command is ignored and error messages are not reported. This is the default.

Example

```
DEFINE SERVER REPORT ERRORS ENABLED
```

DEFINE/SET SERVER RETRANSMIT LIMIT Privilege: P

Use this command to specify the maximum number of times that the server will attempt to re-transmit a message to a LAT service node, when the server receives no acknowledgment messages from the service node.

The value set for this option principally affects network performance. By changing the retransmit limit value, you can manage the efficiency of network. For example, setting a low retransmit limit means that there is less traffic on the network because the server makes fewer attempts to transmit a message to the service node. However, the server may not be able to perform some operations due to a "lack of persistence." A larger retransmit limit means that operations are more likely to be successful, but associated with this is more network traffic because the server makes more attempts to transmit a message to the service node. Thus, you may decide to specify a smaller limit when network performance suffers from heavy use, while lightly loaded networks can support the additional traffic caused by extra retransmission attempts.

A value of 120 is recommended for servers that will have sessions that must go through bridges that have a low link speed.

When the server reaches the retransmit limit, without receiving an acknowledgement from the service node, it disconnects all connected sessions in the virtual circuit to the node.

Syntax

```
DEFINE/SET SERVER RETRANSMIT LIMIT limit
```

Where	Means
limit	The maximum number of times that the server will attempt to re-transmit a message to a service node when the server receives no acknowledgment messages from the service node. Valid values are from 4 to 120. The default value is 8.

Example

```
DEFINE SERVER RETRANSMIT LIMIT 4
```

DEFINE/SET SERVER SOFTWARE Privilege: P

Use the SET command to define the name of the host file containing the access server's software. Use the DEFINE command to change the load file name in the non-volatile RAM.

```
DEFINE SERVER SOFTWARE  <filename>       (DEFINE a Host file)

SET SERVER SOFTWARE SOFTWARE <filename> (Change an existing load file name)
```

DEFINE SERVER RIP STATE Privilege: P

This command performs the same function as the DEFINE SERVER DAEMON ROUTED ENABLED/DISABLED command. It is included for compatibility with Xyplex router products.

The RIP STATE command provides a method for exchanging routing information among gateways or hosts, using the Routing Information Protocol that is defined in RFC 1058. The access server uses this protocol to learn about Internet routes from other hosts or gateways (in this case, the server behaves as though it was a UNIX host). In the Xyplex routed implementation, the server listens for routing messages and updates its internal routing tables, without transmitting any routing information to other gateways or hosts (i.e., the server is a "silent" or "passive" router).

Note that in previous releases, Xyplex servers only updated their internal routing tables by listening to and storing ICMP re-direct messages, or by having routes added by a privileged user via the DEFINE/SET SERVER IP ROUTE command. (These methods are used as well.) Internet routes that are learned via RIP or ICMP re-direct messages are lost when the server is re-initialized. Internet routes learned via RIP expire after 5 minutes, unless the server receives another RIP message with the route. All Internet routes that the server knows can be viewed using the SHOW/LIST/ MONITOR IP ROUTES command

See the UNIX Daemons section in the *Advanced Configuration Guide* for more information. See also the SHOW/MONITOR IP ROUTES command.

You must use the INIT DELAY command to reboot the server before the change can take effect.

Syntax

```
DEFINE SERVER RIP STATE       [ENABLED]
                              [DISABLED]
```

ENABLED Enable RIP on the server.

DISABLED Disable RIP on the server. This is the default.

Example

```
DEFINE SERVER RIP STATE ENABLED
```

DEFINE/SET SERVER RLOGIN Privilege: P

Use this command to specify whether or not users on this server can connect to a UNIX host via the RLOGIN command. Typically, the RLOGIN feature provides a convenient method of logging on to a UNIX host by bypassing the login routine at that host.

See Using TCP/IP Features section of the *Advanced Configuration Guide* for more information.

You must use the INIT DELAY command to reboot the server before the change can take effect. The server must be running TCP/IP in order to use RLOGIN.

Syntax

```
DEFINE/SET SERVER RLOGIN   [ENABLED]
                           [DISABLED]
```

Where	Means
DISABLED	Users on this server cannot connect to a UNIX host via the RLOGIN command. You might want to disable the use of RLOGIN in order to prevent unauthorized users from logging on to the UNIX host, forcing users to log on via the host login routine and supplying a login password.
ENABLED	Users on this server can connect to a UNIX host via the RLOGIN command. This is the default.

Example

```
DEFINE SERVER RLOGIN DISABLED
```

DEFINE SERVER ROTARY ROUNDROBIN Privilege: P

Use this command to choose the type of search: roundrobin or first available, for IP ports mapped to a rotary rather than in sequence, in a "round robin" fashion. This means that ports 1-5 are connected in a rotary of ports 1-7, and then the connection to port 3 went away (so port 3 was now available), then the next connection would use port 3 rather than port 6.

After issuing this command, issue the SHOW/LIST SERVER INTERNET ROTARY command to view the new setting.

You must use the INIT DELAY command to reboot the server before the change can take effect. The server must be running TCP/IP in order to use RLOGIN. There is no SET command for this feature.

Syntax

```
DEFINE SERVER ROTARY ROUNDROBIN     [ENABLED]
                                    [DISABLED]
```

Where	Means
ENABLED	The server searches the IP rotary list in a roundrobin method for the next available port which may not be the lowest. This is the default.
DISABLED	With Rotary Roundrobin disabled, the search begins at the lowest available port.

Example

```
DEFINE SERVER ROTARY ROUNDROBIN DISABLED
```

DEFINE/SET SERVER SCRIPT SERVER Privilege: P

Use this command to specify a TFTP host or MAXserver script server, as well as the directory path where the login script file is located. You can specify up to 4 hosts as script servers. You must designate one or more script servers in order to use the dialback feature.

See the Scripts section of the *Advanced Configuration Guide* for more information.

Syntax

```
DEFINE/SET SERVER SCRIPT SERVER [domain-name "directory-path"]
                                [internet-address "directory-path"]
```

Where	Means
domain-name	The domain-name of a network script server.
internet-address	The internet-address of a network script server.
"*directory-path*"	The name of the directory where script files can be located. A valid *directory-path* can be a string up to 40 characters long. Separate the d*irectory-path* from the *internet-address* or *domain-name* with a space. Enclose the *directory-path* in quotation marks.

Example

```
DEFINE SERVER SCRIPT SERVER 140.179.224.10 "/tftpboot/scripts"
```

DEFINE SERVER SECURID ENABLED/DISABLED Privilege: P

Use this command to enable or disable the SecurID authentication feature on the access server.

SecurID is a system of server software, client software, and accompanying SecurID cards. The system is designed to secure a TCP/IP computer network, preventing unauthorized users from gaining access to resources, but allowing authorized users to gain access easily to these resources.

See the Security Features section of the *Advanced Configuration Guide* for more information about setting up the SecurID client at the Xyplex server.

You must reinitialize the server using the INIT DELAY command for the change to take effect.

Syntax

```
DEFINE SERVER SECURID   [ENABLED]
                        [DISABLED]
```

Where	Means
ENABLED	The SecurID feature can be used on this server.
DISABLED	The SecurID feature cannot be used on this server. This is the factory default.

Example

```
DEFINE SERVER SECURID ENABLED
```

The server responds with a message similar to:

```
-705- Change leaves approximately nnnnn bytes free.
```

DEFINE SERVER SECURID ACMBASETIMEOUT Privilege: P

Use this command to specify how many seconds the SecurID client will wait before prompting the user to supply a PASSCODE.

When a user attempts to log on to a port that requires authentication via SecurID, the port requires that the user specify a PASSCODE which consists of a Personal ID Number (PIN) and a pseudo-random number that is generated by a SecurID card. If the user types an incorrect PASSCODE, the SecurID client will wait for a period of time before prompting the user again to type a PASSCODE. The access server manager can specify the length of the initial period that the SecurID client will wait before prompting the user again. The SecurID software requires that for each incorrect PASSCODE, the client must double the period of time that the user must wait until the client again prompts the user.

See the Security Features section of the *Advanced Configuration Guide* for more information about SecurID.

Syntax

```
DEFINE SERVER SECURID ACMBASETIMEOUT value
```

Where	Means
value	The initial time between prompts for a PASSCODE. A valid value is between 1 and 10 seconds. The default is 3 seconds.

Example

```
Xyplex>> DEFINE SERVER SECURID ACMBASETIMEOUT 5
```

DEFINE/SET SERVER SECURID ACMMAXRETRIES Privilege: P

Use this command to specify how many times the client will attempt to connect to the ACE/Servers in its list for authentication.

When a user attempts to log on to a port that requires authentication via SecurID, the port requires that the user specify a PASSCODE which consists of a Personal ID Number (PIN) and a pseudo-random number that is generated by a SecurID card. The SecurID client then requests authentication from a SecurID server (which is called an ACE/Server). If the first ACE/Server does not respond to an authentication request, the Xyplex client will request authentication from the alternate servers, in order, until it receives a response. If no ACE/Servers respond, the Xyplex client will repeat the process until it reaches the limit.

Syntax

```
DEFINE/SET SERVER SECURID ACMMAXRETRIES value
```

Where	Means
value	Specifies how many times the Xyplex client will attempt to connect to the ACE/Servers in its list of ACE/Servers (SERVER0 through SERVER4) in order to authenticate a user. A valid value is a number between 1 and 10. The default is 5.

Example

```
DEFINE SERVER SECURID ACMMAXRETRIES 4
```

DEFINE/SET SERVER SECURID ACM_PORT Privilege: P

Use this command to specify the UDP port number which the Xyplex access server (the SecurID client) will use when communicating with one or more ACE/Servers. The value you specify for this setting must match the value you specify at one or more ACE/ Servers. The specific setting on the ACE/Server that must match the setting for this command is: acm_port.

Communication between a SecurID client (the Xyplex unit) and server (ACE/Server) are handled using the Internet User Datagram Protocol (UDP). Both the SecurID server and client must be configured with the same SecurID server UDP port number.

Syntax

`DEFINE SERVER SECURID ACM_PORT` *`udp-port number`*

Where	Means
`udp-port number`	The UDP port number to use when sending information to one or more ACE/Servers (SERVER0 through SERVER4) in order to authenticate a user. A valid *udp-port number* is a number between 1 and 1023; the default is 755. This value must match the value for the acm_port parameter specified at any ACE/Servers which the Xyplex client will use to authenticate a user.

Example

```
DEFINE SERVER SECURID ACM_PORT 1023
```

DEFINE/SET SERVER SECURID ENCRYPTION MODE Privilege: P

Use this command to specify the encryption method used. The server supports two encryption methods: DES (Defense Encryption Standard) and SDI Block Cipher (proprietary Security Dynamics Technologies, Inc. encryption method). The value you specify must match the value you specify at one or more ACE/ Servers. The specific ACE/Server setting that must match the setting for this command is: use_des or use_sdi.

All data sent between a SecurID client (the Xyplex unit) and server (ACE/Server) is encrypted. The SecurID server and client must be using the same encryption method.

Syntax

```
DEFINE/SET SERVER SECURID ENCRYPTION MODE [DES]
                                         [SDI BLOCK CIPHER]
```

Where	Means
DES	Specifies DES as the encryption method.
SDI BLOCK CIPHER	Specifies the SDI Block Cipher as the encryption method.

Example

```
DEFINE SERVER SECURID ENCRYPTION MODE SDI BLOCK CIPHER
```

DEFINE/SET SERVER SECURID QUERY LIMIT Privilege: P

Use this command to specify the maximum number of attempts that a user can make, before the port is completely logged off.

When a user attempts to log on to a port that requires authentication via SecurID, the port requires that the user specify a PASSCODE which consists of a Personal ID Number (PIN) and a pseudo-random number that is generated by a SecurID card. If the user types an incorrect PASSCODE, the SecurID client will wait for a period of time before again prompting the user to type a PASSCODE. The access server manager can specify the maximum number of attempts that a user can make before the port is completely logged off.

Syntax

```
DEFINE/SET SERVER SECURID QUERY LIMIT limit
```

Where	Means
limit	The maximum number of times that a user at a Xyplex client can enter a PASSCODE before the Xyplex unit will log out the port. A valid value is a number between 1 and 10. The default is 3.

Example

```
Xyplex>> DEFINE SERVER SECURID QUERY LIMIT 2
```

DEFINE/SET SERVER SECURID SERVER*n* Privilege: P

Use this command to specify the IP addresses or domain names of up to five SecurID servers.

When a user attempts to log on to a port that requires authentication via SecurID, the port requires that the user specify a PASSCODE which consists of a Personal ID Number (PIN) and a pseudo-random number that is generated by a SecurID card. The SecurID client then requests authentication from a SecurID server (which is called an ACE/Server). If the first ACE/Server does not respond to an authentication request, the Xyplex client will request authentication from the alternate servers, in order, until it receives a response. If no ACE/Servers respond, the Xyplex client will repeat the process.

Syntax

```
DEFINE/SET SERVER SECURID SERVERn [internet-address]
                                  [domain-name]
```

Where	Means
SERVER*n*	Represents SERVER0 through SERVER4, which are SecurID authentication servers. SERVER0 is the primary SecurID authentication server. SERVER1 through SERVER4 are alternate SecurID authentication servers.
internet-address	The internet-address of the primary or alternate SecurID authentication servers.
domain-name	The domain-name of the primary or alternate SecurID authentication servers. The default domain-name value for SERVER0 is "securid_0."

Example

```
DEFINE SERVER SECURID SERVER0 192.12.119.12

DEFINE SERVER SECURID SERVER1 ACM_HOST.XYPLEX.COM
```

DEFINE/SET SERVER GROUPS Privilege: P

Use this command to specify LAT groups that can have access to this server. You can permit or restrict access to local LAT services to remote nodes and users. Local services are represented by the groups listed in the *group-list*. See the Security Features section in the *Advanced Configuration Guide* for more information about groups.

Syntax

```
DEFINE/SET SERVER GROUPS          [group-list]      [DISABLED]
                                  [ALL]             [ENABLED]
```

Where	Means
group-list	The group codes that are assigned to local services. When you specify a *group-list* without specifying the ENABLED or DISABLED keyword, the specified *group-list* replaces the current list for the local services.
ALL	All groups are enabled or disabled for the local services that are available on the server.
DISABLED	Remove the groups listed in the *group-list* from the list of groups that are available on the server.
ENABLED	Add the groups listed in the *group-list* to the list of groups available on the server.

Example

```
DEFINE SERVER GROUPS ALL ENABLED
```

DEFINE/SET SERVER SERVICES GROUPS Privilege: P

Use this command to define the group numbers for all local services.

Syntax

```
DEFINE/SET SERVER SERVICES GROUPS [group-list]  [action]
                                  [ALL]
```

Where	Means
group-list	The LAT group numbers that LAT services defined on the access server will allow to connect to these services. The valid values are 0 - 255.
action	ENABLED or DISABLED. You can enable or disable a LAT group from connecting to local LAT services on the access server.
ALL	All groups from 0 - 255 will be allowed to connect to local services.

Example

```
DEFINE SERVER SERVICES GROUPS ALL ENABLED
```

DEFINE SERVER SESSION LIMIT Privilege: P

Use this command to specify the maximum number of user sessions that the server can maintain simultaneously. This setting affects the amount of memory that the server will set aside to support user sessions.

You should be careful to limit this value, as the number of sessions affects other server resources which rely on the server's pool of memory. Depending on your server configuration, your unit may not have sufficient resources to support the number of sessions you specify with this command.

Syntax

```
DEFINE SERVER SESSION LIMIT   [limit]
                              [NONE]
```

Where	Means
limit	The maximum number of active sessions that can be connected simultaneously to all ports on the server. Valid values for limit are from 0 to 255 sessions. The default value is 64.
NONE	The server will support as many active sessions to be connected simultaneously to all ports as memory permits.

Example

```
DEFINE SERVER SESSION LIMIT 100
```

DEFINE/SET SERVER TCP ACK DELAYED Privilege: P

Use this command to cause the server to delay sending TCP ACK packets for small increases in the TCP window size.

Syntax

```
DEFINE/SET SERVER TCP ACK DELAYED   [ENABLED]
                                    [DISABLED]
```

Where	Means
ENABLED	Enable the TCP acknowledged delayed feature.
DISABLED	Disable the TCP acknowledged delayed feature. This is the default setting.

Example

```
DEFINE SERVER TCP ACK DELAYED ENABLED
```

DEFINE/SET SERVER TEXTPOOL SIZE Privilege: P

Use this command to specify the size of the textpool area, which is an amount of memory used by the server. The memory is used to: store the server load image and database parameters; support the features you have enabled to run on the unit; store information about sessions, connection destinations, and the connection queue, etc.; and provide session resources for users (e.g., the typeahead buffer). The server must allocate portions of this memory in order to provide these functions in an efficient manner. Since each site's networking communications needs are different, the software provides the means by which the server manager can direct this allocation.

At initialization time, the software allocates "pools" of memory for specific purposes or to store specific types of data. One important memory pool is called the text pool area. The text pool area is a permanently-allocated area of memory, the size of which is fixed at initialization time. The server stores identification strings for nodes, LAT services, and domain names in the text pool area.

You must reboot the server using the INIT DELAY command before the change can take effect.

Syntax

```
DEFINE SERVER TEXTPOOL SIZE text-pool-size
```

Where	Means
text-pool-size	The total number of bytes of memory that the server will allocate for storing identification strings for nodes, services, locally specified domain names, and learned domain-name Valid values are 8192 to 131070. The default value is 16384.

Example

```
DEFINE SERVER TEXTPOOL SIZE 32768
```

DEFINE/SET SERVER TIME SERVER Privilege: P

Use this command to specify the IP address of the host where the access server gets the time. Use the SHOW SERVER IP command to display the current value.

Syntax

```
DEFINE SERVER TIME SERVER [ENABLED] [ip-address]
                          [DISABLED]
                          [REQUIRED]
```

Note: *You must enable the time server before you can specify the Host IP address. If you leave the time server disabled, the server will get the time from its current source.*

Where	Means
ip-address	The IP address of the host where the time is obtained. The default value is Disabled with a Time Server IP address of 0.0.0.0.
REQUIRED	Only the host defined will be queried for time. On failure, the request for time will be repeated every minute.

Example

```
DEFINE SERVER TIME SERVER ENABLED 140.179.0.192
```

DEFINE/SET SERVER TIMEZONE Privilege: P

Use this command to enable the server to determine the local time, based on the Universal Time (formally called Greenwich Mean Timepassed by the load server, after loading via TFTP. Since the server does not have an internal clock, the local time must be calculated from universal time based on your time zone.

Syntax

DEFINE/SET SERVER TIMEZONE *time*

Where	Means
time	The hours and minutes west of Universal Time. Specify this time using the following format: *hh:mm* *hh* is a one or two digit number which is the hour of the day in 24-hour clock format. Valid values for *hh* are numbers in the range of 00 to 23. *mm* is a two digit number which represents the minutes in the hour. Valid values for *mm* are numbers in the range of 00 to 59.

Example

```
DEFINE SERVER TIMEZONE 12:00
```

See also

```
SET SERVER TIME
```

```
SEFINE/SET SERVER TIME SERVER
```

DEFINE SERVER TN3270 DEVICE Privilege: P

Use this command to create a TN3270 device table or change entries in a TN3270 device table. The access server can maintain up to 20 TN3270 device tables. Before you can create a new device table, you must enable TN3270. Use the DEFINE SERVER PROTOCOL TN3270 ENABLED command to enable TN3270.

Note: *There is no SET command for this feature.*

There are several steps to successfully defining a TN3270 device, they are:

1. Enable the TN3270 protocol
2. Define a TN3270 device to a port
3. Define a TN3270 translation table to a port
4. Define local printer support

See the Setting up TN3270 Terminals section in the *Advanced Configuration Guide* for more information.

Defining TN3270 Devices

The TN3270 device tables contain information that the access server uses to emulate IBM 3270 displays at server ports during TN3270 sessions. The following settings need to be defined for each device table:

- Create a new device using the information from an existing device, then modify the following information in the new device table:
  - The TN3278 type
  - The terminal type
  - The Keymap
  - The Screenmap

Syntax

`DEFINE SERVER TN3270 DEVICE [`*`new-device`*`] CREATE [`*`existing-device`*`] PORT [`*`port number`*`]`

DEFINE SERVER TN3270 DEVICE (continued)

Where	Means
new-device	The name of the new device table. Device table names can consist of up to 8 characters.
CREATE	The server will create the new device table and copy the information from the existing device table or the information defined at PORT n.
existing-device	The server will copy the device information you specify in this variable to create the new device. If this is the first time you have created a new device, the existing devices are ANSI, VT100, VT220-7, and VT220-8.
PORT	The access server will copy the device information defined at the port in the port number variable to create the new device.
port number	The port number the server will use to create the new device.

Modify Entries in the New Device Table

`DEFINE SERVER TN3270 DEVICE [`*`device-name`*`] TERMINAL TYPE [“`*`term-type`*`”]`

Where	Means
device-name	The name of a device table you want to modify. The device you specify can be one of the Xyplex supplied devices or one that you have created.
TERMINALTYPE	Specifies the text description of the terminal type in the *device-name* variable.
"*termtype*"	A text description. Describes the type of terminal in the *device-name* variable. This description can include from 1 to 21 characters, enclosed in quotes.

DEFINE SERVER TN3270 DEVICE (continued)

Example

```
DEFINE SERVER TN3270 DEVICE VT100A TERMINAL TYPE "Don's device table"
```

Define the TN3278TYPE

```
DEFINE SERVER TN3270 DEVICE [device-name] TN3278TYPE [model]
```

Where	Means
TN3278TYPE	Specify the IBM display station type in the *model* variable.
model	An IBM display station type. The are two types: MODEL2 for 24 x 80 display and MODEL5 for 27 x 132 display.

Modify the Keymap

```
DEFINE SERVER TN3270 DEVICE [device-name] KEYMAP [key] [escape-seq] [description]
```

Where	Means
KEYMAP	Specify an IBM display station function in the *key* that will execute at the local terminal when the user enters the key sequence you specify in the "*escape-seq*" variable.
key	An IBM 3270 display station function. See the TN3270 section of the *Advanced Configuration Guide* for a list of IBM display station functions to use in this variable.

"*escape-seq*" The byte sequence from the local terminal that the access server maps to the IBM display station function in the *key* variable. (You specify the local terminal in the *device-name* variable.) You can specify the characters in the byte sequence in two ways: enter the hexadecimal values, which you obtain from your *TN3270 Programmer's Reference manual* for the local terminal, or manually press the keys on the terminal. You can use from 0 to 9 hexadecimal values in this variable, and enclose the variable in quotes.

"*description*" A text description. Describes the keymap escape sequence in different keymap displays. These include SHOW PORT KEYMAP and the display that appears when the user presses the SHOWKEYS status key during TN3270 terminal emulation. You can use up to 5 characters in this variable, and enclose the variable in quotes.

Modify Screenmap Entries

```
DEFINE SERVER TN3270 DEVICE [device-name}  SCREENMAP action "escape-seq" MOVECURSOR
escape-seq [BASE value] SGR [ENABLED/ DISABLED] PORT KEYMAPS [ENABLED/ DISABLED]
```

SCREENMAP Specify a screenmap action that will execute at the local terminal when the user enters the key sequence in the "*escape-seq*" variable.

action A screenmap action. See the TN3270 section of the *Advanced Configuration Guide* for a list of actions to use for this variable. (When you specify MOVECURSOR as the screenmap action, you can optionally specify an offset value (BASE value) for the row and column positions, other than the default, which is 1.)

"escape-seq" The hexadecimal value of the screenmap action. Refer to the Programmer's Reference Manual for the local terminal to obtain this hexadecimal value. Enclose the variable in quotes.

MOVECURSOR You will specify an escape sequence.

BASE You will specify a base value for the MOVECURSOR screenmap action.

value An offset value for the row and column position of the cursor. Valid values are 0 through 255. The default is 1.

SGR You will specify how the server will implement the bold, blink, and underscore screen attributes at the terminal.

ENABLED The server will use the SET GRAPHIC RENDITION command to implement the bold, blink, and underscore screen attributes. This is the default setting.

DISABLED The server will use ON/OFF escape sequences to implement the bold, blink, and underscore screen attributes.

PORT KEYMAPS	You will specify whether or not an individual port can maintain and modify its own copy of a keymap. Note that an additional 1 K of memory is required for each port that uses this feature. The copy of the keymap exists only in the operational database, not the permanent database.
DISABLED	An individual port cannot maintain its own copy of a keymap. This is the default setting.
ENABLED	An individual port can maintain its own copy of a keymap.

Define Alternate Keymapping

```
DEFINE SERVER TN3270 DEVICE [device-name} ALTMAP [name]
```

ALTMAP	The TN3270 device table entry that contains the alternate keymapping.
name	The name of the TN3270 device table entry that contains the alternate keymapping. If you specify NONE as the *name*, you disable any alternate keymap for the TN3270 device. Alternate keymaps let you define multiple sets of input sequences for a terminal keyboard which all map to the same function. See the *Advanced Configuration Guide* for more information.

Examples

The following commands modify the distributed VT100 device and add two alternate keymaps. As a result, the TN3270 function keys PA1-PA3 can also be invoked by the sequences ESC-1 through ESC-3, and Control/A-1 through Control/A-3.

```
DEFINE SERVER TN3270 DEVICE CREATE  VT100

DEFINE SERVER TN3270 DEV VT100 KEYMAP ALTMAP TV925

DEFINE SERVER TN3270 DEV TV925 CREATE EMPTY

DEFINE SERVER TN3270 DEV TV925 KEYMAP PA1 "1B 31" "ESC-1"

DEFINE SERVER TN3270 DEV TV925 KEYMAP PA2 "1B 32" "ESC-2"

DEFINE SERVER TN3270 DEV TV925 KEYMAP PA3 "1B 33" "ESC-3"
```

DEFINE SERVER TN3270 DEVICE (continued)

```
DEFINE SERVER TN3270 DEV TV925 KEYMAP ALTMAP PT250

DEFINE SERVER TN3270 DEV PT250 CREATE EMPTY

DEFINE SERVER TN3270 DEV PT250 KEYMAP PA1 "01 31" "CTRA1"

DEFINE SERVER TN3270 DEV PT250 KEYMAP PA2 "01 32" "CTRA2"

DEFINE SERVER TN3270 DEV PT250 KEYMAP PA3 "O1 33" "CTRA3"
```

DEFINE SERVER TN3270 DEVICE SCREENMAP COLOR Privilege: P

The server supports the two color modes for IBM 3270 terminal emulation: basic 4-color mode and extended 7-color mode. The basic 4-color mode consists of green, red, blue, and white. The extended 7-color mode includes the four basic colors and pink, yellow, and turquoise. The mode you use depends on the colors that your terminal supports as well as those colors that the IBM host application supports.

To use color, you must define the SCREENMAP escape sequence for each color you will use. In addition, you must enable the TELNET TN3270 XTDATTRS (extended attributes) at your port to support the extended 7-color mode.

See the PORT TELNET TN3270 XTDATTRS command for more information. Also see the TN3270 section of the *Advanced Configuration Guide* for details.

Syntax

```
DEFINE SERVER TN3270 DEVICE device-name SCREENMAP COLORxxx  "escape-sequence"
```

Where	Means
port-list	One or more access server ports.
COLORxxx	Indicates which color you want to define an escape sequence for (*xxx* represents the name of a color). Possible colors include: COLORRED COLORGREEN COLORBLUE COLORYELLOW COLORWHITE COLORPINK COLORTURQUOISE
"escape-sequence"	The hexadecimal ANSI-standard escape sequences for these colors. Check the documentation for your terminal if the terminal supports other types of escape sequences. The following is a list of standard escape sequences for various colors. "1B 5B 33 31 6D" ANSI-standard for red "1B 5B 33 32 6D" ANSI-standard for green "1B 5B 33 34 6D" ANSI-standard for blue "1B 5B 33 33 6D" ANSI-standard for yellow "1B 5B 33 37 6D" ANSI-standard for white "1B 5B 33 35 6D" ANSI-standard for pink "1B 5B 33 36 6D" ANSI-standard for turquoise

Example

```
DEFINE SERVER TN3270 DEVICE TV925 SCREENMAP COLORRED "1B 5B 33 31 6D"
```

DEFINE SERVER TN3270 DEVICE KEYMAP NUM_OVERRIDE Privilege: P

Use this command to specify a key to allow alphanumeric data to be entered in a numeric-only field. This command follows all of the standard rules for defining a TN3270 device key.

When the NUM_OVERRIDE is defined, users can toggle this key OFF and ON. It is OFF at the start of any TN3270 session. When the key is ON, the user can enter alpha characters into a numeric-only field. If the status line is activated, the following message displays on the status line: X NUM_OVERRIDE.

Use the SHOW SERVER TN3270 DEVICE command to display the current keymap settings.

SYNTAX

DEFINE SERVER TN3270 DEVICE <*device-name*> KEYMAP NUM_OVERRIDE <*key-sequence*> <*description*>

Where	Means
device-name	The name of the device that the keymap will be created for.
key-sequence	Enter the escape sequence that key will send to the port from the terminal.
description	This is what will display on the SHOW PORT KEYMAP screen for this function.

Example

NEED AN EXAMPLE

DEFINE SERVER TN3270 DEVICE NAME Privilege: P

Use this command to add entries to the TN3270 keymap. This command lets you add additional key mappings for several device types.

Use the SHOW KEYMAP and SHOWKEYS commands to display the defined keymaps.

The PREFIX1 and PREFIX2 function keys allow you to define hex sequences that get prepended to other function keys hex values. The maximum size of the prefix function (1 or 2) is 8 bytes. You can combine 3 keys into the prefix and have those 3 keys prefix the "main" key. When the operator then keys the "main" key, (the one with the FF or FE beginning the hex string), the entire prefix string plus the "main" key is sent to the host.

Syntax

```
DEFINE SERVER TN3270 DEVICE [device-name]     [CREATE] [device-type]
                                              [KEYMAP] [PREFIX1] [bytes]
                                              [KEYMAP] [PREFIX2] [bytes]
                                              [KEYMAP] [PF1] [bytes]
                                              [KEYMAP] [PF2] [bytes]
```

Where	Means
CREATE	The device type the keymap will apply to. The valid values are: ANSI VT100 VT220-7 VT220-8
KEYMAP	You are creating a Keymap.
PREFIX1	This function is prepended to the TN3270 function key that begins with the hex sequence ff.
PREFIX2	This function is prepended to the TN3270 function key that begins with the hex sequence fe.
PF1	The TN3270 function key that is mapped to a hex sequence
PF2	The TN3270 function key that is mapped to a hex sequence
bytes	The hex sequence the TN3270 function is mapped to.

DEFINE SERVER TN3270 DEVICE NAME (continued)

Example

```
DEFINE SERVER TN3270 DEV NAME KEYMAP prefix1 "1b 75"

DEFINE SERVER TN3270 DEV NAME KEYMAP prefix2 "1b 74"

DEFINE SERVER TN3270 DEV NAME KEYMAP PA1 "fe 1b 31"

DEFINE SERVER TN3270 DEV NAME KEYMAP PA2 "ff 1b 32"
```

DEFINE SERVER TN3270 TRANSLATIONTABLE Privilege: P

Use this command to create a TN3270 translation table or change entries in a TN3270 translation table. See the TN3270 section of the *Advanced Configuration Guide* for more information about creating and modifying translation tables.

Syntax

```
DEFINE/SET SERVER TN3270 TRANSLATIONTABLE [new-table] CREATE [existing-table]
TRANSLATIONTABLE [trans-name table  offset value]
```

Where	Means
new-table	The name of a new translation table. Translation table names can consist of up to 8 characters.
CREATE	The server will create the translation table in the *new-table* variable based on the table in the *existing-table* variable.
existing-table	The translation table that the access server will use to create the new translation table. If this is the first time you have created a new translation table, USENGLSH is the name you use in this variable.
trans-name	The name of a translation table that you will modify. You must enter the name of a table you have created in this variable. You cannot modify the USENGLSH table.
table	Which part of the translation table you will modify with a new value, depending on the direction of data flow. The two directions you can use in this variable are:

Direction	**Means**
ASCIITOEBCDIC	Apply the new value to outgoing data from the local terminal to the IBM host.
EBCDICTOASCII	Apply the new value to incoming data from the IBM host to the local terminal.

offset	The value in the translation table you will modify. The hexadecimal values 40 through FF apply to the EBCDICTOASCII part of the table, and the values 20 through FF apply to the ASCIITOEBCDIC part of the table. See the *Advanced Configuration Guide* for a list of these values.
value	The new hexadecimal translation table entry. The values 20 through FF apply to the EBCDICTOASCII part of the table and the values 40 through FF apply to the ASCIITOEBCDIC part of the table. (This is the reverse of the values in the *offset* variable.)

DEFINE SERVER ULI Privilege: P

Use this command to make the UNIX-like user interface available to users on the server. When enabled, users have access to all of the commands listed in the *Using the Xyplex ULI Guide.*

After the interface is enabled on the server, it must be activated for individual ports, by using either the DEFINE PORT ULI command, or by typing the ULI command.

The UNIX-like interface is only available on servers that are running a multi-megabyte image.

You must reboot the server using the INIT DELAY command in order for the change to take effect.

Syntax

```
DEFINE SERVER ULI [ENABLED]
                  [DISABLED]
```

Where	Means
ENABLED	Enable the UNIX-like interface on the server. This is the default.
DISABLED	Disable the UNIX-like interface on the server.

Example

```
DEFINE SERVER ULI DISABLED
```

DEFINE SERVER USE DEFAULT PARAMETERS Privilege: P

Use this command to reboot the unit with the default server and port parameters. If you enable this command, the next time the server is rebooted, the unit will reset to the default parameters and an informational message will display. After the reboot, the setting for this feature will reset to Disabled.

Use the LIST SERVER LOADDUMP CHARACTERISTICS command to display the current setting for this feature, as well as the current IP address for the server as defined in ROMs.

Note: *This command is not available on the Network 9000 720 Access Server. Use the DEFINE CHASSIS SLOT FACTORY DEFAULTS command instead.*

SNMP

The SNMP OBJECT ID: 1.3.6.1.4.33.1.50

The parameter is a reverse-enabled parameter as follows:

Value	Means
1	Disabled
0	Enabled

Syntax

```
DEFINE SERVER USE DEFAULT PARAMETERS [ENABLED/DISABLED]
```

Where	Means
ENABLED	The server will reboot using factory default parameters.
DISABLED	The server will reboot using the current configuration as defined in the parameter file. This is the default setting.

DEFINE/SET SERVER USERDATA DELAY Privilege: P

Use this command to cause the port to delay sending the data to the connection partner after the connection is established.

User data can be passed to the connection partner when a connection is established. A delay in sending the user data may be useful if the port must wait for the remote partner to complete responding, before processing the user data, for example, while waiting for a login prompt from a host.

Syntax

```
DEFINE/SET SERVER USERDATA DELAY delay-value
```

Where	Means
delay-value	How long the port should delay before sending the user data to the connection partner after the connection is established. Valid *delay-values* are 0 to 30 seconds. Each number represents 10 milliseconds. So, for example, the number 30 translates into a delay of 3000 ms, or 30 seconds. The default is 50 (500 ms).

Example

```
DEFINE SERVER USERDATA DELAY 200
```

DEFINE/SET SERVER VERBOSE ACCOUNTING Privilege: P

Use this command to enable or disable Verbose Accounting on the access server. You must enable Verbose Accounting mode to log messages from the UNIX daemons if they are enabled on the access server.

Syntax

```
DEFINE/SET SERVER VERBOSE ACCOUNTING  [ENABLED]
                                      [DISABLED]
```

Where	Means	
ENABLED	Enable	Verbose Accounting mode..
DISABLED	Disable	Verbose accounting mode. This is the default setting.

Example

```
   DEFINE SERVER VERBOSE ACCOUNTING ENABLED
```

DEFINE/SET SERVER VERBOSE PRIORITY Privilege: P

Use this command to specify a value as a filter to determine whether or not to log messages from some software modules in TCP/IP-LAT software V5.1 or greater, such as the UNIX daemons. It logs messages from those modules that submit a priority level equal to or below the priority you specify. It discards messages that submit a greater priority level than the one you specify. This filter affects only SLIP (including compressed SLIP, or CSLIP) and PPP connections, and the following UNIX daemons: LPD, rwhod, fingerd, and routed.

The server continues to log all traditional accounting messages concerning session activity, regardless of the Verbose Priority number.

Syntax

```
DEFINE/SET SERVER VERBOSE PRIORITY priority-type [LOG FACILITY [USER]]
                                                 [LOCAL number]]
```

Where **Means**

priority-type The priority type that the server will use to filter messages from software modules. Valid values are 0 through 7. The default is 5. Assigning a priority value of 7, which is the highest value, will allow the server to log all messages. The following are the meanings of priority-types 0 through 7.

Type	Means
0	A severe condition. The server usually broadcasts priority 0 messages to all users because it can affect their ability to work on the host.
1	A condition that the system manager needs to correct immediately, such as a corrupted system database.
2	A critical condition, such as a hard device error.
3	A software error condition.
4	A warning message.
5	Conditions that are not error conditions, but may require specific procedures to adjust them.
6	Normal, informational messages.
7	Messages that contain information useful for test situations only.

LOG FACILITY USER	The UNIX host will log the accounting information to the UNIX "KERN" facility. This is the default.
LOG FACILITY LOCAL *number*	The UNIX host will log the accounting information to a specific UNIX facility. Valid values are 0 through 7 which correspond to the UNIX facilities local0 through local7. The default is 5 (i.e., local5).

Example

```
DEFINE SERVER VERBOSE PRIORITY 7
```

DEFINE/SET SERVER WELCOME Privilege: P

Use this command to change the text that is displayed to users when they log on to the server.

Syntax

```
DEFINE/SET SERVER WELCOME "message"
```

Where	Means

message	The text message that will display to users when they log on to the server. This text can be up to 80 ASCII characters long. The text must be enclosed in quotation marks ("). The default message is:
	
	`Welcome to the Xyplex Access Server.`
	
	For a Printer server, the default message is:
	
	`Welcome to the Xyplex Printer Server.`

Example

```
DEFINE SERVER WELCOME "BOSTON ACCESS SERVER: Call the MIS Dept at 555-2121
if you experience any problems."
```

DEFINE/SET XPRINTER Privilege: P

Use this command to map access server ports to Novell printer servers.

Use the Novell PCONSOLE utility to create Novell printer servers. (Do not confuse the term Novell printer server with a Xyplex printer server, such as a MAXserver 1450 or 1400A Printer Server unit.) Each of these Novell printer servers can be mapped to a physical port on a access server or printer server. The port can be either a serial port or a parallel port. Each Xyplex access server or printer server port can be connected to only one Novell printer server.

Xprinter support is only provided on Multi-Megabyte load images.

See the *Printer Confirguration Guide* for more information.

Syntax

```
DEFINE/SET XPRINTER [printer-server-name][printer-number]PORTS[port number]
                                                    TERMINALS[terminal-number]
```

Where	Means
printer-server	The name of an Novell NetWare printer server that you set up using the PCONSOLE utility.
printer-number	The number of a Novell NetWare printer that you set up at the Novell printer server (file server) using the Novell PCONSOLE utility. Novell NetWare allows you to specify up to 16 printers, numbered 0 through 15.
port number	The number of the access server and printer server port. Each port can be connected to only one Novell Printer Server.
terminal-number	The terminal number of the access server.

Example

```
DEFINE XPRINTER POSTSCRIPT 6 PORT 4
```

DEFINE SERVER XPRINTER DATA TIMEOUT Privilege: P

Use this command to specify how long an Xprinter print job can idle before Xyplex frees the port.

Syntax

```
DEFINE SERVER XPRINTER DATA TIMEOUT [number]
```

Where	Means
number	The number in seconds that the Xprinter print job can idle. Valid numbers are from 15 to 300 seconds. The default is 15 seconds.

Example

```
DEFINE SERVER XPRINTER DATA TIMEOUT 50
```

DEFINE/SET SERVER XREMOTE FONT SERVER Privilege: P

Use this command to specify the domain name or IP address of the primary or secondary font server. Defining a secondary font server is optional.

The XDM host can be a font server, but you must define it as such. If you have defined both a primary and a secondary font server, the access server requests the file from both servers. It retrieves the file from the font server that responds first.

Syntax

```
DEFINE/SET SERVER XREMOTE [PRIMARY] FONT SERVER    [internet-address]
                          [SECONDARY]              [domain-name]
                                                   [NONE]
```

Where	Means
PRIMARY	The primary font server.
SECONDARY	The secondary font server.
domain-name	The domain name of the font server.
internet-address	The Internet address of the font server. You can specify an IP address of 0.0.0.0 to remove a previously specified IP address.
NONE	Remove a previously specified domain name.

Example

```
DEFINE SERVER XREMOTE PRIMARY FONT SERVER DEV.SUN.COM
```

SET SERVER PARAMETER VERSION Privilege: P

Use this command to specify the version number of the local permanent parameter file. This is useful when the local parameter version number becomes "out of synch" with the version stored at a remote parameter server.

There is no DEFINE setting for this command.

Syntax

```
SET SERVER PARAMETER VERSION number
```

Where	Means
number	The version number of the local permanent parameter file.

Example

```
SET SERVER PARAMETER VERSION 235
```

DEFINE/SET SERVICE — Privilege: P

Use this command to control the operation of and access to LAT services which are available at the access server.

Syntax:

```
DEFINE/SET  SERVICE  [service-name] [characteristic(s)]
```

You can define or set multiple service settings with a single command. When you specify more than one service setting with one command, separate the settings with one or more spaces, a comma, or any combination of commas and spaces. (Note, however, that the maximum length of a command line is 132 characters.)

The following list is a summary of the service settings you can define with this command:

```
[CONNECTIONS]     [DISABLED]
                  [ENABLED]

[IDENTIFICATION]  ["identification-string"]

[PASSWORD]        [password]

[PORTS]           [port-list] [DISABLED]
                  [ALL]       [ENABLED]

 [QUEUE]          [DISABLED]
                  [ENABLED]
```

Where	Means
service-name	The name of the service which is available at the access server.
CONNECTIONS	Whether or not the access server can accept additional connections to the service specified by the service-name. Note that when you issue this command, the status of any connections that are currently formed is not affected.
DISABLED	The access server cannot accept additional connections to the service specified by the service-name.
ENABLED	The access server can accept additional connections to the service specified by the service-name. This is the default setting for CONNECTIONS.
IDENTIFICATION	Define or change the string included in multicast messages that are sent to other access servers in the network that notifies these servers of the availability of the service specified by the service-name.
"identification-string"	The contents of the string which is included in multicast messages. The identification-string can be up to 40 characters in length, and must be enclosed in quotation marks ("). By default, no string is included in multicast messages. To cancel an existing identification-string, specify a null string in quotation marks (i.e., "").
PASSWORD	Define or change the password which a user must supply in order to use the service specified by the service-name.
password	The password that the user must supply in order to use the service specified by the service-name. The password can be between 1 and 16 printable ASCII characters in length.
PORTS	Define or change the port(s) where the service is offered or is no longer offered.
port-list	The port(s) where a service is offered or is no longer offered.
ALL	Specifies that the service, specified by the *service-name*, is offered by all ports, or is no longer offered by all ports.
Disabled	The service, specified by the *service-name*, is no longer offered at the port(s) specified in the *port-list* or all ports.
Enabled	The service, specified by the *service-name*, is offered at the port(s) specified in the *port-list* or all ports. This is the default setting.

Queue	The server will queue a connection request for connection to the service which is specified by the *service-name*.
Disabled	The server will not place requests for connection to the service into the connection queue.
Enabled	The server will place requests for connection to the service into the connection queue. This is the default.

DEFINE/SET PARAMETER SERVER Privilege: P

Use this command to add a specific parameter server to the list of available parameter servers which the access server maintains. The access server will ensure that the parameter information stored at the specified parameter server is kept up to date. Typically, you would use the SET PARAMETER SERVER command after you temporarily removed a parameter server using the CLEAR PARAMETER SERVER command.

The SERVER PARAMETER SERVER LIMIT setting specifies the maximum number of parameter servers that the server can store in a database.

Syntax:

```
DEFINE/SET [SERVER]PARAMETER SERVER node name ADDRESS [ethernet-address]
                                              IP ADDRESS [internet-address]
```

Where	Means
node name	The name of the parameter server to add to the list of parameter servers.
ADDRESS	Identifies the Ethernet address of the parameter server to be added to the list of parameter servers that the access server maintains.
ethernet-address	The unique Ethernet address of the parameter server. Valid values are six pairs of hexadecimal numbers separated by hyphens (e.g., AA-01-04-C9-56-F1).
INTERNET ADDRESS	Identifies the IP address of the parameter server to be added to the list of parameter servers that the access server maintains.
internet-address	The unique IP address of the parameter server.

Example:

```
SET PARAMETER SERVER VAX1 ADDRESS AA-01-04-C9-56-F1

DEFINE PARAMETER SERVER UNIXHOST IP ADDRESS 119.20.112.3
```

DISCONNECT — Privilege: S, N, P

Use the DISCONNECT (or DISCONNECT SESSION) command to terminate one or all sessions to which your terminal is connected. Use the DISCONNECT PORT command to terminate all sessions at a port other than the port which you are logged on to.

You can use the SHOW SESSION display to determine the number(s) of the session(s) you wish to terminate.

Non-privileged and secure users can terminate sessions at the port they are logged on to. Users at privileged ports can use the DISCONNECT PORT to terminate a session at any port.

Syntax:

```
DISCONNECT  [PORT [port-list]SESSION [session-number] ALL
            [SESSION [session-number]
            [ALL]
```

Where	Means
PORT	Terminate all sessions that are connected at a port other than the port you are currently logged on to.
port-list	The number(s) of the access server port(s), other than the port you are currently logged on to, whose access server sessions are to be terminated.
SESSION	Designate a session that will be terminated.
session-number	The number of the session that will be terminated.
ALL	Terminate all sessions to which the port is connected.

Examples:

```
DISCONNECT SESSION 2

DISCONNECT ALL

DISCONNECT PORT 3-5 SESSION ALL
```

```
Xyplex> SHOW SESSIONS

 Port 1:  R. Smith         Service Mode     Current Session 1
 - Session 1: Connected    Interactive      FINANCEVAX
 - Session 2: Connected    Interactive      UNIXVAX
 - Session 3: Connected    Interactive      LASER
```

Sample SHOW SESSION Screen

FORWARDS Privilege: S

Use the FORWARDS command to select the next available, higher-numbered session to which your port or terminal is connected. (The access server assigns a session number for each session to which a port is connected.)

For purposes of the FORWARDS command, the access server tracks session numbers in a "circular" manner. Therefore, when a port is already connected to the highest numbered session, typing FORWARDS connects the port to the lowest numbered port. When only one session is active at a port, the FORWARDS command re-connects the port to that session.

You can use the forward switch character, if one is defined for your port, instead of the FORWARDS command. Refer to the SET PORT FORWARD SWITCH command).

Syntax:

```
FORWARDS
```

Examples:

The following examples illustrate the use of the FORWARDS command. Example 1 is a basic example which shows how to use the FORWARDS command to go from one session to the next higher numbered session. Example 2 is a more complicated example showing how to use the FORWARDS command to connect to sessions from among three different sessions.

1. Suppose that there are two sessions running at a port, and the SHOW SESSION display for this port appears as shown.

```
Xyplex> SHOW SESSIONS

Port 1:  R. Smith         Service Mode     Current Session 1
- Session 1: Connected    Interactive      FINANCEVAX (FINANCEVAX)
- Session 2: Connected    Interactive      UNIXVAX (UNIXVAX)
```

Sample SHOW SESSION Display

As shown in the Sample Show Session Display, the port is connected to two sessions, numbered 1 and 2. Session 1 is the currently active session. If you type the following command:

```
FORWARDS
```

The access server will connect the port to session number 2, and display the message:

```
Xyplex -012- UNIXVAX session 2 resumed
```

The next screen shows the SHOW SESSION display after you issue the FORWARDS command.

```
Xyplex> SHOW SESSIONS

 Port 1:  R. Smith         Service Mode     Current Session 2
 - Session 1: Connected    Interactive      FINANCEVAX (FINANCEVAX)
 - Session 2: Connected    Interactive      UNIXVAX (UNIXVAX)
```

Sample SHOW SESSION Display

2. Suppose that there are three sessions running at a port, and the SHOW SESSION display for this port appears as shown in the following display.

```
 Xyplex> SHOW SESSIONS

 Port 1:  R. Smith         Service Mode     Current Session 1

 - Session 1: Connected    Interactive      FINANCEVAX (FINANCEVAX)
 - Session 2: Connected    Interactive      UNIXVAX (UNIXVAX)
 - Session 4: Connected    Interactive      LASER
```

Sample SHOW SESSION Display

As can be seen in the display, the port is connected to three sessions, numbered 1, 3 and 4. Session 1 is the currently active session. If you type the following command:

```
Xyplex> FORWARDS
```

The access server will connect the port to session number 3, which is the next available higher numbered session. If you return to the Xyplex> prompt and again type:

```
Xyplex> FORWARDS
```

The access server will connect the port to session number 4.

GET CARD LOAD FILE — Privilege: P

Use this command to retrieve a load image from a host on the LAN to a flash card in an access server, either through TFTP or XMOP (use XMOP to get the image from another Xyplex unit).

Syntax

```
GET CARD LOAD FILE [image-name] ADDRESS [ip-address] AREA [area-number]
                                        [ether-address] AREA [area-number]
```

Where	Means
"image-name"	The name of the updated image file
ip-address	The IP address where the image file is located
ether-address	The Ethernet address where the image file is located.
area-number	The area on the flash card where you want to store the file.

Example

```
GET CARD LOAD FILE "xpcsrv20.sys" 140.179.255.110  AREA 2
```

GET CARD STOP Privilege: P

Use this command to terminate the image loading update that was initiated with the GET CARD LOAD FILE command.

Syntax

```
GET CARD STOP
```

HELP — Privilege: P, N, S

Use the HELP command to display on-line information about particular commands. The TCP/IP-LAT software provides a brief explanation, and a summary of command options, for each command that is available to the user.

Privileged users can display help information about all commands. Non-privileged and secure users can only display help information about the commands they are allowed to execute.

Syntax

```
HELP [topic  [keyword [keyword [keyword]]]]
```

Where	Means
topic and keywords	The command(s) or keyword(s) that you need help with. If you enter a single keyword, you will be prompted for the next logical keyword(s) (or sub-topics) that can follow.

Examples

```
HELP SET PORT

HELP SET PORT ACCESS

HELP DEFINE SERVER RADIUS TIMEOUT
```

INITIALIZE SERVER Privilege: P

Use the INITIALIZE SERVER command to reboot the access server, or to cancel a previous INITIALIZE SERVER command. Using the INITIALIZE command, the access server returns to a state which is exactly the same as if you powered up the server (i.e., all settings are restored to the values specified in the permanent database. Values specified using SET commands are reset to the values in the permanent database, users are logged out, and the server image is reloaded).

You can specify a delay period before the access server reboots. When you issue the INITIALIZE command without specifying a delay period, the access server broadcasts a warning to all ports notifying any users who are logged on (the default is 1 minute). If you specify a delay time which is between 2 and 29 minutes, the server will broadcast a warning immediately, and then every minute for each of the last 5 minutes, until re-initialization. If you specify a delay of 30 minutes or greater, the access server will broadcast a message immediately, once every 30 minutes prior to re-initialization, and then once every minute for the last 5 minutes. These messages are broadcast regardless of the BROADCAST setting. Broadcast messages are only displayed at ports that have BROADCAST enabled.

If you specify INITIALIZE DELAY 0,the server will reboot immediately unless there are unsaved parameters, in which case you will receive the "Warning Configuration Not Saved" error message (message 198). If you specify INITIALIZE DELAY *n*, and a user changes a permanent parameter (i.e., uses a Define command) before *n* minutes expire, the initialization is delayed until the parameters are saved. If the parameter server cannot save the parameters, the user who entered the Define command will receive the 198 error message, and the server will not reboot.

Syntax

```
INITIALIZE [SERVER] [DELAY] [delay-time]  [OVERRIDE]
                    [CANCEL]
```

Where	Means
SERVER	An optional keyword.
DELAY	Re-initialization to occur after a specified period of time.
delay-time	How long the server will wait until the re-initialization occurs. Valid values are 0 to 32767 minutes. The default value is 1 minute.

INITIALIZE (continued)

OVERRIDE	The server will perform the initialization even if there are unsaved parameters. If you do specify "OVERRIDE" and parameters have only been partially updated, the parameter file can become corrupted.
CANCEL	Cancel a previously issued INITIALIZE command.

Example

```
INITIALIZE DELAY 1

NITIALIZE SERVER DELAY 5

INITIALIZE SERVER DELAY 5 OVERRIDE

INITIALIZE CANCEL
```

LAT CONNECT — Privilege: S, N, P

Use this command to establish a LAT session by creating a virtual connection between your port (terminal) and a service that is offered at a LAT service node. Most users will use the LAT CONNECT command to establish a session between the port they are logged on to and a host or access server. When you use the LAT CONNECT command, without specifying a service-name, the access server will attempt to establish a session with a preferred LAT service, when one has been defined.

By using the LAT CONNECT command, you require the access server to interpret the command qualifiers as applicable to a LAT service, rather than allowing the server to select a Telnet domain-name that is the same as a LAT service-name.

LAT services can be offered at more than one service node or port. The access server assumes that all services which have the same service-name are equivalent. Therefore, when a service is offered at more than one node or port, the access server will connect to the node or port which has the highest rating (the relative ability to support additional sessions). LAT CONNECT command options permit you to select the particular service node or port, where the service is offered, to which the access server will connect.

Connections to a LAT service are also subject to the following conditions:

1. The port and the device offering the LAT service must have a matching group code.

2. When a service has reached the maximum number of connections it is allowed to have, additional connection requests are entered into a connection queue, if one is enabled.

Syntax

`LAT CONNECT [[SERVICE] service-name] [NODE node name] [DESTINATION port name]`

LAT CONNECT (continued)

Where	Means
SERVICE	An optional keyword. Specifies that you will provide a *service-name*, to which the port will be connected.
service-name	The name of the service to which the port will be connected.
NODE	You will provide the name of the service node at which the service, specified by the *service-name*, is offered. You would use this keyword when a service is offered at more than one service node.
node name	The LAT node which offers the service specified by the *service-name*.
DESTINATION	You will provide the name of the access server port at which the service, specified by the *service-name*, is offered. You would use this keyword when a service is offered at more than one port.
port name	The port on the access server which offers the service specified by the *service-name*.

Examples

```
LAT CONNECT FINANCEVAX

LAT CONNECT LASER NODE MAX5000 DESTINATION PORT_2
```

LAT CONNECT PORT Privilege: P

Use this command to specify the name of a LAT service to which a port (other than the one you are on) will be connected. This can be done either by the LAT CONNECT PORT command, or by defining a dedicated or preferred service for the target port. The PORT ACCESS setting for the target port must be set to LOCAL and the destination port set to REMOTE. The target port cannot have a session in progress (you can terminate an active session using the DISCONNECT PORT command).

Syntax

LAT CONNECT PORT [*port number*][*service-name*][NODE *node name*] [DESTINATION *port name*]

Where	Means
PORT	Connect a target port to a LAT service.
port number	The number of the target access server port that will be connected to a LAT service.
service-name	The name of the LAT service to which the port will be connected.
NODE	Designate a LAT node that offers the service specified by the service-name. You would use this keyword when there are multiple LAT service nodes which offer the service.
node name	The LAT service node that offers the service specified by the service-name.
DESTINATION	Designate an access server port that offers the service specified by the service-name. You would use this keyword when there are multiple ports on an access server that offer the service.
port name	The access server port that offers the service, specified by the service-name.

Example

```
LAT CONNECT PORT 5 LASER
```

LIST

See the SHOW/LIST/MONITOR commands.

LOCK Privilege: S, N, P

Use the LOCK command to secure a terminal (temporarily disable user access to active terminal sessions), without disconnecting your current sessions or logging out. The LOCK command requires that you provide a password (which is not displayed) before the terminal is disabled. To re-enable the terminal, you must enter the correct password. If you forget the password, you must have a user at a privileged port log out that port (which disconnects all current sessions) before the port can be used again.

To use the LOCK command, you must first enable the SERVER LOCK command.

Syntax

```
LOCK
```

Example

When you type the command:

```
Xyplex> LOCK
```

the access server responds with the prompt:

```
Lock Password>
```

Type in a password containing between 1 and 16 characters. The terminal will not display the password on the screen (or printer in the case of a hardcopy terminal). The access server then displays the prompt:

```
Verification>
```

Type the same password. If you correctly type the password, the server will respond with a message and prompt similar to the following:

```
Xyplex - 019 - Port 1 locked
Unlock Password>
```

When you are ready to re-enable the terminal, type the password at the Unlock Password> prompt.

LOGOUT PORT Privilege: S, N, P

Use this command to log off from the access server, or to log out from other ports. LOGOUT PORT also disconnects all sessions.

Note: *All users can log out their own port. Only a user at a privileged port can log out other ports.*

Syntax

```
LOGOUT [PORT]  [port-list]
               [ALL]
```

Where	Means
PORT	Identifies the port which is to be logged off the access server.
port-list	The port(s) which are to be logged off. The default value is your own port.
ALL	Log out all ports from the access server.

Examples

```
LOGOUT
```

```
LOGOUT PORT 5-7
```

MONITOR

All MONITOR commands are described with the SHOW commands.

PURGE DOMAIN — Privilege: P

Use this command to delete one or all *domain-name* entries from the permanent database. You can use the DEFINE DOMAIN command to respecify deleted *domain-name(s)*. If the domain-name is listed in the operational database, it will still be available until the server is re-initialized or it is removed using a CLEAR DOMAIN command. (See also the CLEAR DOMAIN command.)

If the specified *domain-name* is not a fully qualified *domain-name*, it will be concatenated with the default Internet *domain-suffix*. The server will display an error message if you use the PURGE DOMAIN command when the specified Domain name does not exist.

Syntax

```
PURGE DOMAIN   [domain-name]
               [ENTRY entry-number]
               [ALL]
```

Where	Means
domain-name	The local domain name to be removed from the permanent database.
ALL	All domain names will be removed from the permanent database.
ENTRY	Identify, by entry-number shown in the LIST DOMAIN display, the domain-name/internet-address combination that will no longer be available to server users.
entry-number	A line shown in the "Entry" column of the LIST DOMAIN display, which represents a domain-name/internet-address combination that will no longer be available to server users. Note that domain-name entries in the permanent database do not need to match the entries in the operational database. Therefore, if you want to PURGE and CLEAR a domain-name, you should make sure that you have selected the correct entry number.

Examples

PURGE DOMAIN FINANCESUN.XYPLEX.COM

PURGE DOMAIN ALL

```
PURGE DOMAIN ENTRY 5
```

PURGE MANAGER — Privilege: P

Use this command to remove selected network server information.

The CLEAR command is not valid for this feature.

Syntax

```
PURGE MANAGER  [ALL]
               [GLOBAL]
               [LOCAL TYPE] [ALL]
               [LOCAL TYPE] [hardware-type]
               [NODE]
               [PARAMETER]
```

Where	Means
ALL	Remove all entries defined in the client service list. All GLOBAL and NODE entries in the client service list are removed, as well as the parameter files corresponding to defined NODE clients. All LOCAL and NODE entries in the client service list are removed, as well as the parameter files corresponding to defined NODE clients. No load service will be provided until new entries are defined.
hardware-type	The server maintains a client service database to determine which network devices it can service. Database entries can exist as follows: NODE - an individual device. GLOBAL - all devices in the network. LOCAL - all devices in the chassis. A requesting device can be covered by more than one class; if so, its NODE entry supersedes any other entry. GLOBAL entries can optionally be restricted to particular types of equipment. For example, only 8-port access servers. This is selected by the TYPE keyword and a numeric hardware type value for the desired product.

You can define multiple GLOBAL entries to enable service for more than one TYPE of product, or different load image files for each LOCAL entry can optionally be restricted to particular types of equipment. For example, only 20-port access servers. This is selected by the TYPE keyword and a numeric hardware type value for the desired product.

You can define multiple LOCAL entries to enable service for more than one TYPE of product, or to define different load image files for each product.

Examples

```
PURGE MANAGER LOCAL TYPE

PURGE MANAGER GLOBAL

PURGE MANAGER NODE

PURGE MANAGER PARAMETERS
```

PURGE SERVER IP ROTARY Privilege: P

Use this command to delete one or all rotary entries from the permanent database. A rotary is a group of ports on the server that are assigned the same internet address. The deleted rotaries can be respecified using a DEFINE SERVER IP ROTARY command. Since the rotaries are only being deleted from the permanent database, they will remain available until the server is re-initialized or the rotary is removed using a CLEAR SERVER IP ROTARY command.

Examine the LIST SERVER IP ROTARY display to determine the entry number for a particular rotary in the permanent database. Note that rotary entries and their associated entry numbers in the permanent database do not need to match the entries in the operational database. Therefore, if you want to PURGE and CLEAR a rotary, you should make sure that you have selected the correct entry number.

The server will display an error message if you use the PURGE IP ROTARY command when the specified entry does not exist.

Syntax

```
PURGE SERVER IP ROTARY  [entry]
                        [ALL]
```

Where	Means
entry	The entry number of the rotary that will be deleted from the permanent database. This rotary will no longer be available after the server is re-initialized. unless it is re-enabled with a DEFINE SERVER IP ROTARY command.
ALL	All internet-rotaries will be removed from the permanent database. These rotaries will no longer be available after the server is re-initialized, unless the internet-rotaries are re-enabled with a DEFINE SERVER IP ROTARY command.

Example

```
PURGE SERVER IP ROTARY 1
```

PURGE [PORT] IP SECURITY Privilege: P

Use this command to remove one or all entries from the Internet Security table in the permanent database. Once purged, an entry can be respecified using the DEFINE PORT IP SECURITY command. (Also, note that the CLEAR IP SECURITY command is used to remove a security table entry from the operational database

Examine the output of the LIST PORT IP SECURITY command to determine the entry number in the Internet Security table that you want to remove. Note that security entry numbers in the permanent database do not need to match the entries in the operational database. Therefore, if you want to PURGE and CLEAR a security entry, you should make sure that you have selected the correct entry number.

This command clears the security assignment (allow or deny access) for all ports in the *port-list*, for which the assignment was made. To disable Internet Security for a specific port, use the DISABLE option of the DEFINE PORT IP SECURITY command.

The server will display an error message if the entry you specify does not exist.

Syntax

```
PURGE [PORT] IP SECURITY   [entry]
                           [ALL]
```

Where	Means
entry	Corresponds to a number appearing in the Entry field of the LIST PORT IP SECURITY output.
ALL	Purges all entries in the Internet Security table.

Example

```
PURGE PORT IP SECURITY 3
```

PURGE PARAMETER SERVER Privilege: P

Use this command to remove a parameter server from the list of parameter servers that the server maintains in the permanent database. Once purged, the parameter server can be respecified using the DEFINE PARAMETER SERVER command. Also refer to the CLEAR PARAMETER SERVER command, which is used to remove a parameter server from the operational database.

Examine the output of the LIST PARAMETER SERVER command to determine the node name of the parameter server you want to remove.

The server will display an error message if the parameter server you specify does not exist.

Syntax

```
PURGE PARAMETER SERVER node name
```

Where	Means
node name	The node name of the parameter server to be purged, which appears in the output of the LIST PARAMETER SERVER command.

Example

```
PURGE PARAMETER SERVER UNIXSUN
```

PURGE PORT IP SECURITY Privilege: P

Use this command to remove IP security entries for one or more designated port(s) from the permanent database. Once cleared, a permanent database entry can be respecified using the DEFINE PORT IP SECURITY command. The server will display an error message if the entry you specify does not exist. Also refer to CLEAR PORT IP SECURITY command, which is used to remove entries from the operational database.

Syntax

```
PURGE PORT  [port-list] IP SECURITY
            [ALL]
```

Where	Means
port-list	One or more access server ports will be removed from the Internet Security entries stored in the permanent database.
ALL	All security entries on the specified port(s) will be removed.

Example

```
PURGE PORT 4 IP SECURITY
```

PURGE SERVER IP ROUTE Privilege: P

Use this command to delete one or all internet-route entries from the permanent database. The deleted internet-route(s) can be respecified using a DEFINE SERVER IP ROUTE command. Since the internet-route(s) are only being deleted from the permanent database, they will remain available until the server is re-initialized or the route is removed using a CLEAR SERVER IP ROUTE command.

Examine the LIST SERVER IP ROUTE display to determine the entry number for a particular internet route in the permanent database. Note that internet-route entries in the permanent database do not need to match the entries in the operational database. Therefore, if you want to PURGE and CLEAR an internet-route, you should make sure that you have selected the correct entry number.

The server will display an error message if you use the PURGE SERVER IP ROUTE command when the specified entry does not exist.

Syntax

```
PURGE SERVER INTERNET ROUTE   [entry]
                              [ALL]
```

Where Means

entry The entry number of the internet-route that will be deleted from the permanent database. This internet-route will no longer be available to server users after the server is re-initialized, unless the route is re-enabled with a DEFINE SERVER IP ROUTE command.

ALL All internet-routes will be removed from the permanent database. These entries will no longer be available to server users after the server is re-initialized, unless the internet-routes are re-enabled with a DEFINE SERVER IP ROUTE command.

Examples

```
PURGE SERVER IP ROUTE 1

PURGE SERVER IP ROUTE ALL
```

PURGE SERVER MENU Privilege: P

Use this command to remove an item on the server's menu from the permanent database. Once purged, the menu item can be respecified using the DEFINE SERVER MENU command. (See also the CLEAR SERVER MENU command, which is used to remove a menu item from the operational database.)

Examine the output of the LIST SERVER MENU command to determine the number of the entry that you want to remove.

The server will display an error message if the entry that you specify does not exist.

Syntax

```
PURGE SERVER MENU item-number
```

Where	Means
item-number	The item number (1 - 20) within the menu that you want to remove.

Example

```
PURGE SERVER MENU 3
```

PURGE SERVER SCRIPT SERVER Privilege: P

Use this command to delete one or all script server entries from the permanent database. The deleted script servers can be respecified using a DEFINE SERVER SCRIPT SERVER command. Since the script servers are only being deleted from the permanent database, they will remain available until the server is re-initialized or the script server is removed using a CLEAR SERVER SCRIPT SERVER command.

Examine the LIST SERVER SCRIPT SERVER display to determine the entry number for a particular script server in the permanent database. Note that script server entries in the permanent database do not need to match the entries in the operational database. Therefore, if you want to PURGE and CLEAR a script server, you should make sure that you have selected the correct entry number.

The server will display an error message if you use the PURGE SERVER SCRIPT SERVER command when the specified entry does not exist.

Syntax

```
PURGE SERVER SCRIPT SERVER [entry]
                           [ALL]
```

Where	Means
entry	The entry number of the script server which will be deleted from the permanent database. This script server will no longer be available after the server is re-initialized unless it is re-enabled with a DEFINE SERVER SCRIPT SERVER command.
ALL	All internet-script servers will be removed from the permanent database. These script servers will no longer be available after the server is re-initialized, unless the internet-script servers are re-enabled with a DEFINE SERVER SCRIPT SERVER command.

Examples

```
PURGE SERVER SCRIPT SERVER 1
```

```
PURGE SERVER SCRIPT SERVER ALL
```

PURGE SERVER TN3270 DEVICE Privilege: P

Use this command to delete a TN3270 device table from the permanent database. Before it deletes the table from the database, the access server checks that the table is not being used by a port. The server will not delete a table that is currently in use. TN3270 device tables exist only in the permanent database, so Clear commands do not apply to them. Examine the SHOW/LIST SERVER TN3270 display to determine the TN3270 devices in the permanent database.

If you delete *all* of the device tables in the database, the access server will re-enable the Xyplex-supplied tables (ANSI, VT100, VT220-7, and VT220-8) after the server is re-initialized.

The server will display an error message if you use the PURGE SERVER TN3270 DEVICE command when the specified device does not exist, or when it is in use by a TN3270 port.

Syntax

```
PURGE SERVER TN3270 DEVICE [device-name]
```

Where	Means
device-name	The name of the of the TN3270 device table that will be deleted from the permanent database.

Example

```
PURGE SERVER TN3270 DEVICE VT100
```

PURGE SERVER TN3270 TRANSLATIONTABLE Privilege: P

Use this commandto delete a TN3270 translation table from the permanent database. Before it deletes the table from the database, the access server checks that the table is not being used by a port. The server will not delete a table that is currently in use. TN3270 translation tables exist only in the permanent database, so Clear commands do not apply to them. Examine the SHOW/LIST SERVER TN3270 display to determine the TN3270 translation tables in the permanent database.

The access server does not allow you to delete the default table, USENGLSH, that Xyplex supplies with the software. You can only delete tables that you have created on the server with the DEFINE SERVER TN3270 TRANSLATIONTABLE command.

The server will display an error message if you use the PURGE SERVER TN3270 TRANSLATIONTABLE command when the specified entry does not exist, or when it is in use by a TN3270 port, or if you attempt to delete the USENGLSH table.

Syntax

```
PURGE SERVER TN3270 TRANSLATIONTABLE [trans-name]
```

Where	Means
trans-name	The name of the of the TN3270 translation table that will be deleted from the permanent database. This translation table will no longer be available after the server is re-initialized. You can only delete tables that you have created. You cannot delete USENGLSH, the Xyplex-supplied translation table.

Example

```
PURGE SERVER TN3270 TRANSLATIONTABLE SPANISH
```

PURGE SERVICES Privilege: P

Use the PURGE SERVICES command to delete, from the permanent database, the entry for one or all of the LAT services offered locally at the server. Use the DEFINE SERVICE command to respecify the deleted service. Since services are only being deleted from the permanent database, they will still operate until the next time the server is re-initialized, unless they are removed by a CLEAR SERVICES command.

Syntax

```
PURGE SERVICES [service-name]
               [LOCAL]
```

Where	Means
service-name	The name of the LAT local service (e.g., a service which is offered by the server) which will no longer be offered by the server.
LOCAL	All local LAT services (e.g., services which are offered by the server) will no longer be offered by the server.

Examples

```
PURGE SERVICE LOCAL
```

```
PURGE SERVICE LASER
```

PURGE XPRINTER PORTS Privilege: P

Use this command to delete, from the permanent database, the entry for the Novell printer services offered at one or more terminal or Xyplex printer server ports. Use the DEFINE XPRINTER command to respecify the deleted Novell printer service. Since the services are only being deleted from the permanent database, they will still operate until the next time the server is re-initialized, unless they are removed by a CLEAR XPRINTER PORTS command.

Syntax:

```
PURGE XPRINTER PORTS [port-list]
                     [ALL]
```

Where	Means
port-list	Remove the permanent database entry for the Novell printer services offered at one or more terminal or Xyplex printer server ports.
ALL	Remove the permanent database entry for the Novell printer services offered at all ports which offer this service.

Example

```
PURGE XPRINTER PORTS 1,3-5
```

REFRESH SERVER CCL NAME Privilege: P

CCL scripts are ASCII text files which contain commands that specify initialization and operational characteristics for the specific type of modem that is connected to a port. CCL scripts are stored at script servers (hosts which can transfer a file to the server via TFTP). Individual ports can be configured to use a specific CCL script using the DEFINE PORT CCL NAME command.

Occasionally, you may want to change the contents of a CCL script and then make the server load that CCL script. The REFRESH SERVER CCL NAME command causes the server to re-load the CCL script. Ports that are currently running the CCL script of that name will continue to execute the old version of the script until they exit.

Xyplex supplies a number of CCL scripts for use with a variety of modems that can be connected to either the communication server serial port or to the Macintosh computer.

Refer to the documentation supplied with APDA Modem Tool Kit for a description of the CCL script language. See the Scripts section of the of the *Advanced Configuration Guide* for a description of how to configure and use script servers.

Syntax

```
REFRESH SERVER CCL NAME "ccl-name"
```

Where	Means
ccl-name	The name of the CCL script to be loaded at ports which use that script.

Example

```
REFRESH SERVER CCL NAME "SupraFAXModem_V.32bis"
```

Additional Notes

When you issue the REFRESH SERVER CCL command, if there are any syntax errors in the CCL script, the server will report the number of the line in the script which is in error, and a description of the problem. The following table lists the possible error messages:

REFRESH SERVER CCL NAME (continued)

Message	Comments/Corrective Action
Memory allocation failure	There is insufficient free memory left on the server to run the CCL script. Refer to the Flash Cards & Memory information for some strategies to resolve this problem.
Unknown instruction name	A bad instruction was contained in the CCL script. Check for the syntax of the command in the documentation supplied with APDA Modem Tool Kit.
Message	**Comments/Corrective Action**
Value out of range	An illegal argument value was contained in the CCL script. Check for the syntax of the command in the documentation supplied with APDA Modem Tool Kit.
Argument missing	Command requires an argument that is missing. Check for the syntax of the command in the documentation supplied with APDA Modem Tool Kit.
Illegal backslash expresson in string	In a CCL script, the Backslash (\) character can only be followed by one of the following: • two decimal digits the \ character the ^ character Refer to the documentation supplied with APDA Modem Tool Kit for more information.
Numeric argument expected	A numeric value was expected but not found. Check for the syntax of the command in the documentation supplied with APDA Modem Tool Kit.
String exceeds maximum length	A text string that was too long was found in the CCL script. The maximum length of a text string is 255 characters. Check for the syntax of the command in the documentation supplied with APDA Modem Tool Kit.
@ANSWER entrypoint missing @HANGUP entrypoint missing @ORIGINATE entrypoint missing	One of these mandatory commands was missing from the CCL script. Check for the syntax of the command in the documentation supplied with APDA Modem Tool Kit.

REMOTE CONSOLE Privilege: P

Use the REMOTE CONSOLE command at one local access server unit, to connect and log on to the console port of a remote server unit. The remote server unit must support the Remote Console Facility. (Many LAT devices support this facility, although some do not, and others like the DECsa access server support it in an incompatible manner). After the remote console session has been formed, you can issue server unit commands for the remote server unit, just as though you were directly to that server unit.

If there is a maintenance password defined for the remote server unit you wish to log on to, you will be required to supply that password in order to use the REMOTE CONSOLE command. Failure to supply the password will prevent a remote connection from being formed, but this failure will appear as though the server has not responded. See the DEFINE SERVER MAINTENANCE PASSWORD command for more information.

The Console LED remains lit whenever there is either a local or remote console session. To terminate the remote console session, type the <BREAK> character or local switch character (tilde ~ is the default) in order to return to the local server's command prompt, then issue the DISCONNECT command.

There are several pre-defined port settings (i.e., PORT SPEED) for the remote console port of the remote server unit, when a remote console session has been established. You cannot change the following settings:

Feature	Setting	Feature	Setting
ACCESS	LOCAL	INPUT FLOW CONTROL	ENABLED
AUTOBAUD	DISABLED	INPUT SPEED	9600
BREAK	DISABLED	MODEM CONTROL	DISABLED
CHARACTER SIZE	8	OUTPUT FLOW CONTROL	ENABLED
DEDICATED SERVICE	NONE	OUTPUT SPEED	9600
DIALUP	DISABLED	PARITY	NONE
DSRLOGOUT	DISABLED	PASSWORD	ENABLED
DTRWAIT	DISABLED	SPEED	9600
FLOW CONTROL	XON		

REMOTE CONSOLE (continued)

Syntax

```
REMOTE CONSOLE [NODE node name] [MAINTENANCE [PASSWORD] password]
[ethernet-address] [MAINTENANCE [PASSWORD] password]
```

Where	Means
NODE	Identify the *node name* of the remote server unit to which a remote console session will be established. ***NOTE**: When connecting to a server remote console port by specifying a node name, the target server must offer at least one LAT local service. If the target server does not offer a local service, you must specify the Ethernet address of the target server in order to establish a remote console connection.*
node name	The name of the server unit where a remote console session will be established.
ethernet-address	The unique Ethernet address of the remote server unit. Valid values are in the form of six pairs of hexadecimal numbers which are separated by hyphens (e.g., AA-01-04-C9-56-F1).
MAINTENANCE PASSWORD	You will supply the maintenance password for the remote server unit.
"password"	The maintenance password for the remote server unit. The password is a hexadecimal number in the range of 0 to FFFFFFFFFFFFFFFF (i.e., up to 16 hexadecimal digits). The password must be in quotation marks ("). The default is 0. The maintenance password at the remote server unit was set using a DEFINE SERVER MAINTENANCE PASSWORD command.

Examples

```
REMOTE CONSOLE NODE MX1620

REMOTE CONSOLE NODE MX1620 MAINT PASSWORD "9C"
```

```
REMOTE CONSOLE AA-01-C4-11-73-F8 MAINT PASS "9C"
```

Example of initiating and exiting from a remote console session:

This is an example of how you initiate and exit from a session from within a remote console session.

1. Issue the REMOTE CONSOLE command. For example:

   ```
   REMOTE CONSOLE AA-01-C4-11-73-F8 MAINT PASS "9C"
   ```

2. Press the <RETURN> key until the server unit responds with the login prompt (#).

The # prompt (the login password prompt) indicates that you must enter the login password. (The actual password prompt on your server unit may be different, because the server manager can assign a new prompt.) Obtain the login password from the server manager. The login password is not the same password as the maintenance password used in the REMOTE CONSOLE command.

3. Enter the login password and press the <RETURN> key. When you type the correct login password, the server unit will display the Enter username> prompt.

4. At the Enter Username> prompt, type a username and press the <RETURN> key. You can specify a username that is between 1 and 16 characters long, or type a <CTRL>/<Z> command to automatically assign a username for the port (the assigned username is in the form: PORT_n). The username helps the server manager identify the port where you are logged on, in case there are problems.

   The unit will now display the local command prompt. For example:

   ```
   Xyplex>
   ```

   (The local command prompt on your server unit may be different.) When you see the local command prompt, you are logged on to the remote console port. You can enter all server commands from the local command prompt.

5. Terminate the remote console session by typing the <BREAK> character or local switch character. This will return you to the local command prompt from where you initiated the remote console. Type the DISCONNECT command to complete termination of the remote console session. (You could also use the RESUME command to continue the remote console session.)

REMOVE QUEUE Privilege: P

Use the REMOVE QUEUE command to delete requests for connection to LAT local services from the access server connection queue.

Syntax

```
REMOVE QUEUE   [ENTRY entry-number]
               [NODE node name]
               [SERVICE service-name]
               [ALL]
```

Where	Means
ENTRY	You will remove the specific entry from the connection queue.
entry-number	The number of the connection queue entry that you wish to delete. Use the SHOW QUEUE command to display a list of queue entries to determine the entry-number.
NODE	Specifies that you wish to remove from the connection queue all connection requests from a specific node.
node name	The name of the node whose connection requests will be deleted.
SERVICE	Specifies that you wish to remove from the connection queue all connection requests to a specific local service.
service-name	The name of the local service whose connection queue entries will be deleted.
ALL	All connection requests will be deleted from the access server connection queue.

Example

```
REMOVE QUEUE ENTRY 1

REMOVE QUEUE NODE FINANCEVAX

REMOVE QUEUE SERVICE LASER

REMOVE QUEUE ALL
```

RESET PORT Privilege: P

Use the RESET PORT command to clear a parallel port that has stopped (i.e.,"hung."). This will allow the next print job in the queue to begin printing.

Note: *This command is available for MX 1400 and MX 1450 print servers only.*

Syntax

```
RESET PORT port-list
```

Where	Means
port-list	One or more parallel ports on a Xyplex printer server that are to be cleared.

Example

```
RESET PORT 3
```

RESUME — Privilege: S, N, P

Use the RESUME command to return to a session that you have exited. If you issue a RESUME command, without specifying the session you wish to resume, the access server will place you back in the current session. Use the SHOW SESSIONS command to display a list of your connected sessions.

You can enter a string of up to 32 characters with the RESUME command. The access server sends this string to the application on the host where you have established a session. The string can contain caret ^ control sequences that the access server converts to actual control characters before it sends them to the application. For example, you might need to include an ^M^J sequence at the end of a character string to send the Carriage Return and Line Feed characters.

The server does not save the character string in multiple RESUME commands. You enter the string each time you want to send it to the application in the RESUME command.

Syntax

```
RESUME   [SESSION session-number] ["character-string"]
         [service-name]
         [domain-name]
         [internet-address]
```

Where	Means
SESSION	You will indicate a particular session number, as displayed on the SHOW SESSIONS screen.
session-number	The session that you wish to resume. The default value is the current session.
service-name	The name of the service with which you wish to resume a session. If there are multiple sessions to the same service-name, the session with the lowest number will be the one that is resumed.
domain-name	The domain name with which you wish to resume a session.
internet-address	The internet address with which you wish to resume a session.
"*character-string*"	A string of up to 32 ASCII characters, including caret control characters which the server will send to the connection partner when the session is resumed. The access server converts caret control characters to actual control characters before it sends them to the application. Enclose the character string in quotes.

Examples

```
RESUME 140.179.240.62 “^M^J”

RESUME SESSION 3

RESUME FINANCEVAX
```

RLOGIN — Privilege: S, N, P

Use this command to logon to a remote host system by specifying the host system and a username that is recognized by the host. The access server passes either the username of the port or the username specified on the RLOGIN command line to the host. Depending on how the RLOGIN implementation at the host is set up, this may be sufficient to allow the user to bypass the login routine of the host (e.g., the user will automatically be logged on to the host, without having to supply a username and password.).

There are advantages and disadvantages to using RLOGIN rather than Telnet to make connections. At some hosts, the RLOGIN implementation can be more efficient at terminating display of output from a program (i.e., when you issue a <CTRL>/<C> command, the user prompt is displayed faster with an RLOGIN connection than a Telnet connection). However, since the RLOGIN protocol is not an Internet-standard protocol, RLOGIN is less widely available and is usually not as well implemented as Telnet. For example, the RLOGIN protocol does not typically support binary session modes, local echoing, or features that are equivalent to the Telnet features such as passing 7-bit CSI escape sequences, and the Telnet "are you there?" and "synchronize" commands. (Refer to the descriptions of the PORT TELNET BINARY SESSION MODE, TELNET ECHO MODE, TELNET CSI ESCAPE, TELNET QUERY, and TELNET SYNCHRONIZE characteristics, respectively).

See the Configuring RLOGIN Support section of the *Advanced Configuration Guide* for a description of the RLOGIN Support feature.

Syntax

```
RLOGIN   domain-name [[USERNAME] "username"]
         internet-address [[Username] "username"]
         NONE
```

Where	Means
domain-name	The domain-name of the host you will log on to.
internet-address	The IP address of the host you will log on to.
USERNAME	An optional keyword. Specifies that you want to enter a username rather than using the port's username.
"username"	Enter a quoted string representing a username that will be recognized by the host.
NONE	The server will connect the port to the preferred service that is defined for that port.

RLOGIN (continued)

Examples

```
RLOGIN UNIXSUN

RLOGIN 140.179.240.61 “ADMINONLY”
```

SCRIPT Privilege: N, P

Use this command to have the port download a script from a script server and perform the commands contained in the script file.

See the Using Scripts section of the *Advanced Configuration Guide* for more information about using scripts.

Syntax

```
SCRIPT "script-name"
```

Where	Means
"script-name"	The name and directory location of the script file to be executed. The file and directory location must be specified as a UNIX-style filename. For example, /usr/login. Enclose the *script-name* in quotation marks ("). The maximum length of the script file name and directory location is 64 characters. With this command, the defined script sever path is ignored - you must provide an explicit path.

Example

```
SCRIPT "/usr/login"
```

SET - General Information

Use the access server SET commands to specify or change settings for ports or terminals, servers, services, sessions, domain names, and user privilege levels, in the operational database. When you use the SET command, the access server's permanent settings are not changed. The port parameters will return to the permanent setting after the port is logged out, and the SERVER parameters revert to the stored configuration when the access server is re-initialized. Use the DEFINE command to create permanent settings.

SET DOMAIN

Refer to the description of the DEFINE/SET DOMAIN commands.

SET PORT

Refer to the description of the DEFINE/SET PORT commands.

SET SERVER

Refer to the description of the DEFINE/SET SERVER commands.

SET SERVER CHASSIS

This command is for the Network 9000/ 720 Access Server. Refer to the Network 9000 documentation for further information.

SET SERVER COPY

Use this command to copy a file from one area to another.

Note: *The Access Server must have a flash card installed in order to use this command.*

Syntax

```
SET SERVER COPY <filename1> <filename2> AREA <area>
```

Where	Means
filename1	The name of the original file.
filename2	The name of the duplicate file.
AREA	You are indicating which area of the card you are copying the file to.
area	The area of the card where the file will be copied.

Note: *Use the SHOW MANAGER FILE command to display the card information.*

EXAMPLE

```
SET SERVER COPY xprcs20.sys xprcs20.sys AREA 2
```

SET SERVER TIME — Privilege: P

Use this command to set or change specify the time that is maintained by the server.

Note that the access server does not have an internal clock. The load host supplies the default time that is maintained by the unit. This command is useful when time changes occur, such as the change to Daylight Savings Time.

Syntax

```
SET SERVER TIME hh:mm:ss
```

Where	Means
hh:mm:ss	Use the following format. Separate each item in the time with a colon.
	hh is two-digit number which is the hour of the day in 24-hour clock format. Valid values are 00 to 23.
	mm is a two-digit number which represents the minutes in the hour. Valid values are 00 to 59.
	ss is a two-digit number which represents the seconds in the minute. Valid values are 00 to 59.

Example

```
DEFINE SERVER TIME 01:00:23
```

See also

```
DEFINE/SET SERVER TIMEZONE

DEFINE/SET SERVER TIME SERVER
```

SET SERVICE

Refer to the description of the DEFINE/SET SERVICE commands.

SET NOPRIVILEGED

Refer to the description of the SET PRIVILEGED/NOPRIVILEGED commands.

SET PARAMETER SERVER

Refer to the description of the DEFINE/SET PARAMETER SERVER commands.

SET PRIVILEGED/NOPRIVILEGED Privilege: P

Use this command to specify the privilege status of the port at which the command is issued. More than one port on an access server can be privileged. Any user who knows the privileged password can use the SET PRIVILEGED command.

When you issue this command, you are required to supply the privileged password. The privileged password is set via the DEFINE/SET SERVER PRIVILEGED PASSWORD command. The factory default privileged password is SYSTEM.

The local command mode prompt changes to indicate that the port is a privileged port (unless the command is issued from a console port). For example, the default local command mode prompt for a non-privileged port is Xyplex>. The default local command mode prompt for a privileged port is Xyplex>>.

See the Password And User Names section of the *Basic Configuration Guide* for more information.

Syntax

SET [PRIVILEGED]
[NOPRIVILEGED]

Where	Means
NOPRIVILEGED	The port will return to non-privileged status. This means that the user will only be able to change parameters for the current port or session. This is the default privilege level when connecting to a port.
PRIVILEGED	The port will have privileged status. This means that the user at the port can set or change operational and permanent parameters for the server, and any or all ports, sessions, or services. When the port is logged out, it will automatically return to a non-privileged status for the next user.

Example

```
SET PRIVILEGED
```

The port displays the Password prompt: Password>

Type the privileged password (password is not echoed by the terminal). The default password is "ACCESS". The access server will then display the privileged local command prompt.

```
Xyplex>>

Xyplex>> SET NOPRIV

Xyplex>
```

SET SESSION Privilege: S, N, P

Use this command to alter the data transparency of the current session. Transparency refers to how the port interprets control characters.

This applies to both LAT and Telnet sessions. For Telnet sessions, when you set the SESSION characteristic to PASSALL or PASTHRU, the access server will attempt to negotiate the Telnet binary option.

When the user has finished using the Telnet binary mode and the session successfully negotiates out of binary mode, the access server software automatically changes the session type to INTERACTIVE.

Syntax

```
SET SESSION [INTERACTIVE]
            [INTERACTIVE_NOIAC]
            [LIMIT]
            [PASSALL]
            [PASTHRU]
            [TRANSPARENT]
```

Where	Means
INTERACTIVE	Enable all switch characters, Telnet command characters, server messages, and XON/XOFF flow control (if the SET PORT FLOW CONTROL is set to XON). Typically, this is the normal mode when a terminal is connected to the port.
INTERACTIVE_ NOIAC	Acts like Interactive mode, but does not process or send any Telnet options.
PASSALL	Disable all switch characters, Telnet command characters, server messages, and XON/XOFF flow control. In PASSALL mode, all characters are passed to the connection partner as data. This allows data files that contain control character to be transferred without interference from the access server. Typically, you would use this mode for binary file transfers (e.g., transferring a program via modem). PASSALL session
LIMIT	Limit the total number of simulatenous sessions the server can support.

PASTHRU	Disable all switch characters, Telnet command characters, server messages, but leave XON/XOFF flow control enabled. Typically, you would use this mode for ASCII file transfers (e.g., printing on a line printer connected to a port).
TRANSPARENT	The server will initially set all sessions so that a Telnet session will ignore Telnet option messages received from a remotely initiated session and will not send any Telnet option messages from the locally initiated session, in addition to disabling all switching characters, Telnet command characters, and XON/XOFF flow control recognition. For a LAT session, the server tells its partner it is PASSALL but acts locally as if it were PASTHRU.

Examples

```
SET SESSION PASTHRU
```

SHOW/LIST/MONITOR - General Information

Use LIST, MONITOR, and SHOW commands to display information about the access server and resources (such as nodes, parameter servers, ports, services, sessions, queues, and users) about which the access server maintains information. The following table describes each of these commands:

Command	**Function**
LIST	Displays information about values contained in the permanent database.
MONITOR	Displays continuously updated information about values contained in the operational database or the current running status.
SHOW	Displays information about values contained in the operational database, or displays a "snapshot" of the current running status.

The SHOW and LIST commands produce "static" displays of the requested information. These displays can be viewed on ANSI and non-ANSI terminals (including hard-copy devices). The MONITOR command generates a display that is continuously updated on the terminal display screen. It is best to set the port to ANSI mode to monitor a screen (see DEFINE/SET PORT TYPE). This will cause the server to repaint the display starting at the top of the screen, making it easier to read. To exit from a MONITOR display:

- Press any key to terminate the display at the end of the current screenful of information.
- Press the <BREAK> key to terminate the display immediately.

For many displays, the first few lines of the display (the "header" lines) contain some fields that are common to each other. For example, the first line of the SHOW SERVER display contains the common fields that are described in the following table.

MaxServer V*x.y*	The Xyplex product type and the version of the access server software, where *x.y* indicates the major and minor software release level.
Rom *xxxxxx*	The version, *xxxxxx*, of access server ROM software.
HW *xx.yy.zz*	The version of the access server hardware. For chassis-type modules, *xx* indicates the version of the access server cards, *yy* indicates the type of chassis, and *zz* indicates the chassis version.
Lat Protocol V*x.y*	The version of the LAT protocol running on the access server, where *x.y* indicates the major and minor protocol release level.
Uptime	How long the access server has been running since it was last initialized. The time is expressed as: `days hours:minutes:seconds.`

SHOW/LIST/MONITOR - General Information (continued)

Address	The unique Ethernet address of the access server.
Name	The name of the access server.
Number	The number of the access server. :

Valid Show, List and Monitor Commands:

Option	Show	List	Monitor
ACCOUNTING	X	—	X (P)
ARAP	X	X	—
CARD STATUS	X	—	X
CCL	X	—	
CHASSIS (Network 9000 720 Access Server only)	X	X	X
COUNTERS	X	—	X (P)
DESTINATIONS	X	—	X (P)
DOMAIN	X	X	X (P)
INTERNET	X	X	X (P)
IP	X	X	X (P)
LOADDUMP CHARACTERITICS	—	X	X (P)
LPD COUNTERS	X	—	X (P)
LPD QUEUE	X (P)	X (P)	X (P)
LPD STATUS	X	—	X (P)
NODES	X	—	X (P)
PARAMETER SERVER	X	X	X (P)
PORTS	X	X	X (P)
QUEUE	X	—	X (P)
RADIUS	X	X	X (P)
SCRIPT SERVER	X	X	X (P)
SERVER	X	X	X (P)
SERVICES	X	X	X (P)
SESSIONS	X	—	X (P)
TERMINALS	X	X	X (P)
UNIT	X	X	X (P)
XPRINTER	X	X	X
XPRINTER PORTS	—	X	—
XPRINTER TERMINALS	—	X	—
MANAGER	X	X	X
MANAGER FILES	X	X	X (P)
MANAGER STATUS	—	—	X (P)

(P) - Privileged users. — Not available.

SHOW/MONITOR CARD STATUS — Privilege: S, N, P

Use this command to display the card's current settings.

Syntax

```
SHOW/MONITOR CARD STATUS
```

Example

```
Xyplex > show card status
TS/720 V6.1 Rom 4C0000 HW 00.02.00 Lat Protocol V5.2 Uptime 0 10:25:35
Address:08-00-87-02-58-64   Name:X025864           Ethernet:A   Number:    0
                                                                 04 Dec 1998  12:44:11

Card Status:    Formatted / Write Enabled
Card Type:      Xyplex / FLASH2 / 2097152 bytes
Device Type:    Intel / 65536 bytes
Card State:     Idle

Get File Host:
Get File Name:
Get File Area:

Get File Current State:    Idle
Get File Previous Status:  None

Parameter Area Updates:    25

Xyplex>
```

SHOW/MONITOR CARD STATUS(continued)

Field	Description
Card Status:	Formatted and write enabled.
Card Type:	Flash = SERIES 1
	Flash 2 = SERIES 2
	Size of Flash card
Card State:	Idle
Device Type:	Manufacturing and size of ROM chips on the Flash card.
Get File Host:	Where you get file from.
Get File Name:	Name of file.
Get File Area:	Area of flash card to put file.
Get File Current State:	What the card is currently doing.
Get File Previous State:	Did previous GET FILE succeed.
Parameter Area Updates:	How many times the PARAM Area of the Flash card was updated since the server was rebooted.

SHOW/LIST/MONITOR CHASSIS

This command is valid for Network 9000/720 Access Servers only. Refer to the Network 9000 documentation for details.

SHOW/MONITOR DESTINATIONS — Privilege: See Below

Use the SHOW DESTINATIONS or MONITOR DESTINATIONS command to display a list of all accessible *domain names* and *service-name*s on the network. The list will be displayed in alphanumeric order. The SHOW DESTINATIONS command produces a static display. The MONITOR DESTINATIONS command produces a display that is continuously updated.

Privileges

Secure and non-privileged users can use the SHOW DESTINATIONS command. Only users at privileged ports can use the MONITOR DESTINATIONS command

Syntax

```
SHOW/MONITOR DESTINATIONS  [name]
```

Where	Means
name	The *domain names* and/or *service-names* on the network you wish to view. This allows you to view one or a limited number of destinations, rather than the complete list. You can specify a wildcard character to select a subset of the destinations to be displayed. The asterisk symbol (*) is the wildcard character. For example, if one types SHOW DESTINATIONS AB*, the server will display all accessible *domain names* and/or *service-names* whose names start with AB. SHOW DESTINATIONS A*BC displays accessible *domain names* and/or *service-names* whose names start with A and end with BC.

Example

```
Xyplex>> SHOW DESTINATIONS

MAXserver V6.0.4S10 Rom 470000 HW 00.01.00 Lat Protocol V5.2  Uptime:  1 18:32:57

DEVVAX                                The Development/Library VAX
GOOFY                                 140.179.240.14
FINANCEVAX                            Corporate MicroVAX II
MAX_1620                              XYPLEX MAXserver 1620
UNIXHOST.COM                         140.179.240.183
```

Sample SHOW/MONITOR DESTINATIONS Display

After the header line, the first column of the SHOW/MONITOR DESTINATIONS display lists accessible domain names and service-names. The second column lists either the internet-address to which the domain-name is mapped, or the identification string for the service-name, which is informational text about the LAT service.

SHOW/MONITOR/LIST DOMAIN Privilege: See Below

Use the SHOW DOMAIN or MONITOR DOMAIN command to display information about one or all available domain names locally, set or defined on the server, or learned by the server. The SHOW DOMAIN command produces a static display. The MONITOR DOMAIN command produces a display that is continuously updated.

Use the LIST DOMAIN command to display information about domain names that are defined in the permanent database of the access server.

Privileges

Secure and non-privileged users can use the SHOW DOMAIN and LIST DOMAIN commands. Only users at privileged ports can use the MONITOR DOMAIN command.

Syntax

```
SHOW/MONITOR/LIST DOMAIN   [domain-name]
                           [ALL]
                           [LEARNED]
                           [LOCAL]
```

Where	Means
domain-name	The access server will display the requested information for the Domain specified by the *domain-name*. If you do not specify a *domain-name*, the display will show all available *domain names* from the relevant database. If you do not specify a fully-qualified *domain-name*, the specified name will be concatenated with the default Internet *domain-name-suffix(es)*. You can specify a wildcard character to select a subset of the *domain names* to be displayed. The asterisk symbol (*) is the wildcard character. For example, if one types SHOW DOMAIN AB*, the server will display all available *domain names* which start with AB. SHOW DOMAIN A*BC displays available *domain names* which start with A and end with BC.
ALL	The access server will display information for *domain names* that it obtained from the primary or secondary Domain name server, as well as those that were specified locally (i.e., using a SET/DEFINE DOMAIN command). This is the default for the LIST/MONITOR/SHOW DOMAIN commands.

LEARNED — The access server will display information about the domain-name(s) that it obtained from the primary or secondary Domain name server.

LOCAL — The access server will display information about domain names that were specified locally (i.e., using a SET/DEFINE DOMAIN command).

Example

```
Xyplex> SHOW DOMAIN

Entry Internet                      Domain     19 Oct 1998 08:23:58
      Address         TTL Source    Name

1     192.112.119.100 100 Primary   UNIXHOST.COM
2     192.112.119.200  24 Secondary FINANCESUN.COM
3     140.179.240.183     Local     MAX1620.COM
4     140.179.240.14      Local     GOOFY
```

LIST/MONITOR/SHOW DOMAIN Display

The following table describes each of the fields on the LIST/MONITOR/SHOW DOMAIN display.

Field	Description
Entry	The entry number assigned by the software for the *domain-name.*
Internet Address	The Internet address of the node.
TTL	The length of time, in minutes (exception: in hours for MX-TSERV-J8 and MX-TSRVL-J16 units), that the access server will retain information about the *domain-name(s)* that it obtained from the primary or secondary Domain name server. This is called "time to live." Locally defined *domain names* have no time to live.
Source	Where the *domain-name* information was obtained. The possible values are:
	Local — The domain-name was specified locally (i.e., using a SET/DEFINE DOMAIN command).
	Primary — The access server obtained information about the domain-name from the primary Domain name server.
	Secondary — The access server obtained information about the domain-name from the secondary Domain name server.
Domain Name	Shows the *domain-name.*

SHOW/LIST/MONITOR PORT LINE EDITOR CHAR Privilege: See Below

Use these commands to display the current settings of the line editing characters for the specified port(s).

Privilege:

Secure and non-privileged users can use LIST or SHOW PORTS commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORTS command.

Syntax

SHOW/LIST/MONITOR PORT [*port-list*] LINE EDITOR CHARACTERISTICS

Note: *If a character is not defined, the server will display "None."*

Example

```
Xyplex> SHOW PORT LINE EDITOR CHARACTERISTICS

Port 4:  Don's Toy                                    17 Nov 1998  19:07:21

                       Line Editor Characters

Backspace Character:           ^D     Forwards Character:          ^F
Delete Beg Character:          ^U     Delete Line Character:       ^X
End of Line Character:         ^E     Begin Line Character:        ^H
Previous Line Character:       ^B     Next Line Character:         ^N
Quoting Character:             ^V     Insert Toggle Character:     ^A
Cancel Character:              ^Z     Redisplay Character:         ^R

MX1620>
```

Field	Description
Backspace Character	The line editing character that will move the cursor one position to the left. The default setting is ^E.
Delete Beg Character	The line editing character that will delete everything on the current command line, from the cursor position to the beginning of the line. The default setting is ^U.
End of Line Character	The line editing character that will place the cursor at the end of the current command line. The default setting is ^E.
Previous Line Character	The line editing character that will recall the previous command in the command history. The default setting is ^B.

SHOW/LIST/MONITOR PORT LINE EDITOR CHAR (continued)

Quoting Character	The line editing character that will quote the next character. The default setting is ^V.
Cancel Character	The line editing character that will cancel an interactive operation (such as changing a password), or delete the current command line. The default setting is ^Z.
Forwards Character	The line editing character that will move the cursor one position to the right. The default setting is ^F.
Delete Line Character	The line editing character that will delete the current command line. The default setting is ^X.
Begin Line character	The line editing character that will place the cursor at the beginning of the command line. The default setting is ^H.
Next Line Character	The line editing character that will recall the next command in the command history. The default setting is ^N.
Insert Toggle Character	The line editing character that alternates between the insert character and overstrike character modes of operation. the default setting is ^A.
Redisplay Character	The line editing character that will redisplay the current command line. The default setting is ^R.

SHOW/LIST/MONITOR MANAGER Privilege: N, S, P

Use the SHOW, LIST or MONITOR MANAGER commands to display all or specific types of server manager information.

Syntax

```
SHOW/LIST/MONITOR MANAGER [CHARACTERISTICS]
                          [CLIENTS]
                          [FILES]
                          [GLOBAL TYPE]   <number>
                                          [ALL]
                          [NODE NAME]     <name>
                          [NODE ADDRESS] <hex-number>
                          [NODE HARDWARE ADDRESS] <hex-number>
                          [STATUS]
```

Where	Displays
CHARACTERISTICS	The current settings for all network server parameters.
CLIENTS	All client selection entry information.
FILES	The name, date and version of all files located on the local flash card.
GLOBAL TYPE	The global and loading information for a specific Xyplex device type. See the latest *Access Server Release Notes* for a listing of all Xyplex device types.
GLOBAL ALL	The global and loading information for all Xyplex device types.
NODE NAME	All loading and dumping information for a specific node.
node name	The node name of the server you want to display. Use the SHOW PARAMETER SERVER or the SHOW NODES ALL command to display the node name.
NODE ADDRESS	Loading and dumping information for a specific Node address.
NODE HARDWARE ADDRESS	The loading and dumping information for a specific node by hardware address.
hex-number	The hexadecimal number specifying the MAC address of a particular Xyplex device.
STATUS	The current operational state of the network load and dump storage servers.

Examples

```
SHOW MANAGER NODE HARDWARE ADDRESS 08-00-87-03-34-6B
```

```
MX1620 V6.0.4 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 3 05:14:11
Address:   08-00-87-03-34-6B   Name:   X03346B              Number:     0

Ethernet Address  Device  Name             Load file    Diag file    Load Dump
08-00-87-03-34-6B  117                     xpCSRV20.SYS              Yes  No
MX1620>
```

SHOW MANAGER NODE ADDRESS Display

```
SHOW MANAGER FILES
```

```
MX1620 V6.0.4 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 3 04:28:04
Address:   08-00-87-03-34-6B   Name:   X03346B              Number:     0

Files from directory /MC/SYSTEM

 File Name    Version   Date        Time         Size
 MCFFS1.SYS   V2.12     16 Mar 1998 18:05:58    28800 bytes AREA 1 Size   64856
 XPCSRV20.SYS V6.0.4    16 Mar 1998 18:06:28   757888 bytes AREA 2 Size 1506833
     2 files, 786688 bytes.

Files from directory /MC/PARAM

 File Name    Version   Date        Time         Size
 -03346B.SYS  ver 101C9 09 Nov 1998 15:49:26    13096 bytes
 DEFAULTS.SYS ver 0     16 Mar 1998 18:04:54     1024 bytes
     2 files, 14120 bytes.
```

SHOW MANAGER FILES Display

```
SHOW MANAGER GLOBAL ALL
```

```
MX1620 V6.0.4 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 3 04:29:08
Address:   08-00-87-03-34-6B   Name:   X03346B              Number:     0

Ethernet Address  Device  Name             Load file    Diag file    Load Dump
Global Devices        76                   xpcsrv20                  Yes   No
Global Devices        86                   xpcsrv20                  Yes   No
Global Devices       117                   xpcsrv20                  Yes   No
Global Devices       119                   xpcsrv20                  Yes   No
Global Devices       120                   xpcsrv20                  Yes   No
Global Devices        92                   xpcsrv20                  Yes   No
```

SHOW MANAGER GLOBAL ALL Display

SHOW MANAGER STATUS

```
MX1620 V6.0.4 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 3 04:58:48
Address:   08-00-87-03-34-6B   Name:   X03346B              Number:     0

Load operations completed:         0   Dump operations completed:         0
Currently Loading:                 0   Currently Dumping:                 0
Total service offers sent:         1   Currently saving parameters:       0
Parameter server status:        Idle

Ethernet Address  Function Version  Seq   Left     File
```

SHOW MANAGER STATUS Display

SHOW/MONITOR NODES — Privilege: See Below

Use the SHOW NODES or MONITOR NODES command to display information about one or all available Ethernet nodes on the network. The SHOW NODES command produces a static display. The MONITOR NODES produces a display that is continuously updated. Note that the SHOW/MONITOR NODES commands do not display information about Telnet nodes.

Privileges

Secure and non-privileged users can use the SHOW NODES command, however, these users are restricted to viewing information about nodes which are in their authorized groups. Users at privileged ports can view information about any available nodes, regardless of the authorized groups for the port, but only the nodes that are offering services in group codes that are defined or set for the server (e.g., if a service node on the network is offering a service in group-code 12, but the server's authorized groups do not include group-code 12, then even a privileged user will not see those services). Only users at privileged ports can use the MONITOR NODES command.

Syntax

```
SHOW/MONITOR NODES      [node name] [COUNTERS]
                                    [STATUS]
                                    [SUMMARY]
```

Where	Means
node name	Display the requested information for the service node specified by the node name.
ALL	Display the requested information for the all service nodes that match the authorized group list for the current port.
COUNTERS	Display statistics about current node activity for the specified node or all nodes.
STATUS	Display detailed status information about the availability of the specified node or all nodes, as well as information about the node Ethernet address, group codes, services offered, etc.
SUMMARY	Display a one-line summary for the specified node or all nodes that match the authorized groups for the current port. This is the default display type.

Examples

```
Node: DON1600                                    08 Oct 1998  01:49:07

Seconds Since Zeroed:          132      Multiple Node Addresses:            0
Messages Received:               0      Duplicates Received:                0
Messages Transmitted:            0      Messages Re-transmitted:            0
Slots Received:                  0      Illegal Messages Received:          0
Slots Transmitted:               0      Illegal Slots Received:             0
Bytes Received:                  0      Solicitations Accepted:             0
Bytes Transmitted:               0      Solicitations Rejected:             0
```

Sample MONITOR/SHOW NODES COUNTERS Display

The following table describes each field on the MONITOR/SHOW NODES COUNTERS display. The values listed below indicate cumulative values counted since the last time the display counters were reset to zero. There are two ways to reset these counters: use a ZERO COUNTERS command, or re-initialize the unit.

Field	Description
Node	The name of the node.
Seconds Since Zeroed	The number of seconds since the counters were reset to zero.
Messages Received	The number of LAT virtual circuit messages that the access server received from the node, since the counters were reset to zero.
Messages Transmitted	The number of LAT virtual circuit messages that the access server transmitted to the node, since the counters were reset to zero.
Slots Received	The number of slots that the server received from the node (where a slot represents a message segment for a particular session), since the counters were reset to zero.
Slots Transmitted	The number of slots that the server transmitted to the node, since the counters were reset to zero.
Bytes Received	The total number of bytes contained in datagrams that have been successfully received by the access server, excluding Ethernet header and CRC data, since the counters were reset to zero.
Bytes Transmitted	The total number of bytes contained in datagrams that have been successfully transmitted by the access server, excluding Ethernet header and CRC data, since the counters were reset to zero.
Multiple Node Addresses	The number of times that a node multicast an announcement on the network, with a physical address that was different from the physical address given in a previous announcement, since the counters were reset to zero.

Duplicates Received	The number of duplicate messages that the server received from the node, since the counters were reset to zero.
Messages Re-transmitted	The number of messages the server retransmitted to the node, since the counters were reset to zero.
Illegal Messages Received	The number of illegally formatted messages that the server received from the node, since the counters were reset to zero.
Illegal Slots Received	The number of illegally formatted slots that the server received from the node, since the counters were reset to zero.
Solicitations Accepted	The number of connection requests that the server has accepted from the node, since the counters were reset to zero. This number includes both queued requests and requests that were immediately satisfied.
Solicitations Rejected	The number of connection requests from the node that the server has rejected, since the counters were reset to zero.

```
Xyplex>> SHOW NODES DON1600 STATUS
Node: DON1600                          Address:  AA-00-04-00-63-E4
LAT Protocol:     V5.2                 Data Link Frame Size:  1500

Identification: Xyplex Access Server/Littleton

Node Groups: 0

Service Name        Status   Rating  Identification

DON1600             Available    83  Xyplex Access Server/SQA Lab
```

MONITOR/SHOW NODES STATUS Display

The following table describes each field on the MONITOR/SHOW NODES STATUS display:

Field	Description
Node node name	The name of the service node.
LAT Protocol Vx.y	The version number (x) and the update level (y) of the service node software LAT protocol.
Address	The Ethernet address of the service node.

Data Link Frame Size	The maximum Ethernet data link frame size used by the service node to receive messages.
Identification	The identification text string for the node.
Node Groups	The group codes enabled for the service node.
Service Name	Each entry in this column shows the name of a service offered on the service node.
Status	Each entry in this column shows the status of the service (listed in the Service Name column) offered by the service node. Valid values for this column are:

Available	The service is currently available to server users.
Reachable	The node is currently accessible to server users, although there are currently no active sessions.
n Connected	The service is available, and that n currently active sessions with this service were requested.
Unavailable	All service nodes offering the service are currently unreachable.
Unknown	The service was available but now may be unavailable. This could be because the server has not recently received a multicast announcement from the service node.

Rating	The value assigned to the service by the node, which indicates the relative capacity of the service to accept new connections. A higher number implies that the node is more able to accept connections. The range of values that is displayed is 0 through 255.
Identification	A text string that identifies the service.

```
Xyplex>> SHOW NODES ALL SUMMARY


Node Name           Status       Identification

DON1600             Reachable    Xyplex Access Server/SQA Lab
ENGWESTPRINT-1      Reachable    Printer Controller in location 2166
ESC-1450            Reachable    Xyplex Printer Server
MILLER_1620         Reachable    Xyplex Access Server MAXserver 1620
NMSQAMAX4           Reachable    Xyplex Access Server
SSEALP              Reachable      SSE Dec 3000 Alpha / OpenVMS AXP
X014ECD             Reachable    Xyplex Access Server/MAXserver 1640
X0170AE             Reachable    Xyplex Access Server/MAXserver 1640
X01C324             Reachable    Xyplex Access Server/MAXserver 1604
X025864             Reachable    Xyplex Access Server/MAXserver 1608B
X0275E2             Reachable    Xyplex Access Server/MAXserver 1640
X027606             Reachable    Xyplex Access Server/MAXserver 1620
X0277B8             Reachable    Xyplex Access Server
X03346B             Reachable    Xyplex Access Server
X047141             Reachable    Xyplex Access Server/MAXserver 1620
X04740F             Reachable    Xyplex Access Server
X04AA48             Reachable    Xyplex Access Server/MAXserver 1620
X09D911             Reachable    Xyplex X25 Gateway
X0AD05C             Reachable    Xyplex Access Server
```

MONITOR/SHOW NODES SUMMARY Display

The following table describes the fields on the MONITOR/SHOW NODES SUMMARY display:

Field	Description
Node	The name of the service node.
Status	Each entry in this column shows the status of the node listed in the Node Name column. Valid values for this column are: *n* Connected — The node is reachable, and that *n* sessions are currently active with services offered by the service node.

	Reachable	The node is currently accessible to server users, although there are currently no active sessions.
	Requesting	A node that does not currently offer services, has made remote connection requests to the server for access to local services offered at the server.
	Unknown	The node was available but now may be unavailable. This could be because the server has not recently received a multicast announcement about the services which are offered at the node.
	Unavailable	An active session has timed out or that the service node is currently unreachable.
Identification	A text string which identifies the node.	

SHOW/LIST/MONITOR PARAMETER SERVER Privilege: See Below

Use these commands to display information about current parameter servers (nodes which store parameter information) for the access server. Use the LIST PARAMETER SERVER command to display information about parameter servers assigned in the permanent database. The SHOW and LIST PARAMETER SERVER commands produce a static display. The MONITOR PARAMETER SERVER command produces a display that is continuously updated.

Privileges

Non-privileged users can use the SHOW or LIST PARAMETER SERVER command. Only users at privileged ports can use the MONITOR PARAMETER SERVER command.

Syntax

```
SHOW/LIST/MONITOR PARAMETER SERVER
```

Example

```
Xyplex>> SHOW PARAMETER SERVER

MX1620 V6.0.4S10 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 1 18:32:36
Address:   08-00-87-03-34-6B   Name:   X03346B              Number:     0

Check Timer:                        30       Parameter Server Limit:         4
Retransmit Timer:                    5       Parameter Servers:              4
Retransmit Limit:                    3       Rejected Servers:               2
                                             Bad Parameter Messages:         0
Path:

Last Update Version:             DD7A        Storage State:                Idle
Last Update Date:          06 Oct 1998       Loaded From:    08-00-87-03-34-6B
Last Update Time:             13:57:34                                  X03346B

Name             Address            Version Date              Status   Reason
Local MemCard    08-00-87-03-34-6B      DD7A 06 Oct 1998 13:57 Current
Local NVS        08-00-87-03-34-6B      DD7A 06 Oct 1998 13:57 Current
GOOFY            140.179.240.14         DD7A 06 Oct 1998 00:13 Current
140.179.240.183  140.179.240.183        DD7A 06 Oct 1998 13:57 Current
```

Sample MONITOR/SHOW PARAMETER SERVER Display

SHOW/LIST/MONITOR PARAMETER SERVER (continued)

The following table describes each field on the MONITOR/SHOW PARAMETER SERVER display (except the header lines, which are described in SHOW/LIST/MONITOR - General Information):

Field	Description
Check Timer	How often (in minutes) the access server attempts to locate additional eligible parameter servers.
Retransmit Timer	How often (in minutes) the access server attempts to update parameter information at a parameter server that does not acknowledge the attempt.
Retransmit Limit	The number of times the access server attempts to update parameter information at a parameter server that does not acknowledge the attempt, after the Retransmit Timer period expires.
Path	The complete directory pathname to be used when writing parameter files via TFTP.
Parameter Server Limit	The maximum number of parameter servers about which the access server will retain information.

Parameter Servers	The current number of parameter servers about which the access server has information.
Rejected Servers	The number of parameter servers which have not acknowledged an attempt to update parameter information by the access server.
Bad Parameter Messages	The number of corrupt parameter messages received by the server.
Path	The path to where the parameters are stored on a remote host.
Chassis Parameter Status	Display on Network 9000/720 Access Server only.
Last Update Version	The version number of the parameter file that is stored in the memory of the access server, since it was last initialized. The access server creates a new version of the parameter file when parameters are changed using the DEFINE or PURGE commands.
Last Update Date	The date when the access server last successfully updated parameter information that is stored at parameter servers.
Last Update Time	The time of day when the access server last successfully updated parameter information that is stored at parameter servers.
Storage State	Whether or not the access server is attempting to update parameter information at any parameter servers. Idle indicates that the access server is not currently attempting an update (this is a normal storage state). All other storage states indicate that an update is being attempted or is in progress.
Loaded From:	The Ethernet address or *internet-address* of the unit from which the server obtained its parameters. The Nodename or *domain-name* of this unit is shown below the Ethernet address or *internet-address*.
Name	The name of a current parameter server.
Address	The unique Ethernet address or *internet-address* of a current parameter server.
Version	The version number of the parameter file that is currently stored at the parameter server. When this number matches the version indicated by the Last Update Version number, the parameter server and the access server have the same version of the parameter file.

Date

The date and time when the parameter server was last updated or when the server made an attempt to update the parameter server.

Status

The status of attempts by the access server to update parameter information at this parameter server. The possible status values are:

Ahead — The parameter server is storing a newer version of the parameter file than the version that is in access server memory.

Behind — The parameter server is storing an older version of the parameter file than the version that is in access server memory.

Current — The parameter server is storing the same version of the parameter file as the one in access server memory.

Failed — The access server has failed in attempting to update the parameter information stored at this parameter server (i.e., the parameter server retransmit limit has been reached). The server will attempt to update this parameter server the next time a user issues any DEFINE or PURGE command, or the CHECK PARAMETER SERVER command.

Failing — The access server has not yet successfully updated the parameter information stored at this parameter server (i.e., the parameter server retransmit limit has not been reached but the attempt has not yet been successful).

Reason — Shows the reason why the Status column shows an update attempt as Failed or Failing. The possible values that can be shown here are:

Invalid — the server has received an invalid (incorrect or corrupted) parameter file from the parameter server.

Open — the software cannot open the parameter file.

Protocol — a protocol error occurred during the update.

Reads — an error occurred while reading the parameter file.

Resource — the parameter server has a resource problem (e.g., insufficient disk space, memory, etc).

Response — the parameter server has not responded.

Writes — an error occurred while writing to the parameter file.

SHOW/LIST/MONITOR PORT ACCESS — Privilege: See Below

Use this command to display information about all ports that have the same ACCESS setting.

Privilege:

Secure and non-privileged users can use LIST or SHOW PORTS commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORTS command.

Syntax

```
SHOW/LIST/MONITOR PORTS   [port-list] ACCESS  [DYNAMIC]
                                              [LOCAL]
                                              [REMOTE]
                                              [NONE]
                                              [PRT3270]
```

Where	Means
port-list	The port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.
ACCESS	Display the requested information for all ports that match the requested ACCESS setting. See the DEFINE/SET PORT ACCESS command description.
DYNAMIC	Display the requested information for all ports set to DYNAMIC.
LOCAL	Display the requested information about all local ports.
REMOTE	Display the requested information about all remote ports.
NONE	Display the requested information about all ports that are not set for any type of access (i.e., cannot be accessed locally or remotely).
PRT3270	Display the requested information about all TN3270 printer ports.

SHOW/LIST/MONITOR PORT ACCESS (continued)

Example

```
XYPLEX> SHOW PORT ACCESS LOCAL

Port    Access    Status        Services Offered        17 Nov 1998  18:50:58

  1     Local     Idle
  3     Local     Wait Input
  4     Local     Executing Cmd
  6     Local     Idle
  7     Local     Idle
  8     Local     Idle
  9     Local     Idle
 11     Local     Idle
 12     Local     Idle
 13     Local     Idle
 14     Local     Idle
 15     Local     Idle
 16     Local     Idle
 17     Local     Idle
 18     Local     Idle
 19     Local     Idle
 20     Local     Idle

MX1620>
```

SHOW/LIST/MONITOR PORT ACCESS Display

SHOW/LIST/MONITOR PORT ALT CHARACTERISTICS Privilege: See Below

Use these commands to view the current values or settings for certain port settings that are not displayed on the SHOW/LIST/MONITOR PORTS CHARACTERISTICS display.

Privilege

Secure and non-privileged users can use LIST or SHOW PORTS commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORTS command.

Syntax

```
SHOW/LIST/MONITOR PORTS   [port-list]ALTERNATE CHARACTERISITCS
                          [ALL]
```

Where	Means
port-list	The port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.
ALL	Display the requested information for all ports on the server.
ACCESS	Display the requested information for all ports that match the requested ACCESS characteristic. See the DEFINE/SET PORT ACCESS command description.
	DYNAMIC Display the requested information for all ports set to DYNAMIC.
	LOCAL Display the requested information about all local ports.
	REMOTE Display the requested information about all remote ports.
	NONE Display the requested information about all ports that are not set for any type of access.

SHOW/LIST/MONITOR PORTS ALTERNATE CHARACTERISTICS (continued)

Example

```
Xyplex>> SHOW PORT ALTERNATE CHARACTERISTICS

MX1620> sh po alt cha

Port 4:  aa                                          17 Nov 1998  18:50:08

Resolve Service:          Any_Lat     DTR wait:                     Disabled
Idle Timeout:                   0     Typeahead Size:                    128
SLIP Address:             0.0.0.0     SLIP Mask:           255.255.255.255
Remote SLIP Addr: 140.179.245.148     Default Session Mode:     Interactive
TCP Window Size:              256     Prompt:                         MX1620
DCD Timeout:                 2000     Dialback Timeout:                  20
Stop Bits:                      1     Script Login:                 Disabled
TCP Keepalive Timer:            0     Username Filtering:               None
Nested Menu:              Disabled     Nested Menu Top Level:             0
Command Size:                  80     Clear Security Entries:       Disabled
Rlogin Transparent Mode: Disabled     Login Duration:                    0
Xon Send Timer:                 0     TCP Outbound Address:         0.0.0.0
Slip Autosend:            Disabled     Radius Accounting:            Disabled
APD Prompt:                Enabled


Username Prompt:          Enter username>
Password Prompt:     Enter user password>
```

LIST/MONITOR/SHOW PORT ALTERNATE CHARACTERISTICS Display

SHOW/LIST/MONITOR PORTS ALTERNATE CHARACTERISTICS (continued)

The following table describes each of the fields on the LIST/MONITOR/SHOW PORT ALTERNATE CHARACTERISTICS display

Field	Description
Port *n*	The number of the access server port about which the system is displaying information. The variable *n* represents the number of a physical access server port.
user-name	The text which follows the port number shows either the name given by the user to log on to the port, or the name given to the port using SET/DEFINE PORT USERNAME.
Resolve Service	How the access server should interpret ambiguous variables in CONNECT commands, DEFINE/SET PORT PREFERRED SERVICE, or DEFINE/SET PORT DEDICATED SERVICE commands. The possible values are: ANY — The server should interpret the variable first as a LAT service-name, then try to interpret it as a Telnet domain-name or internet-address. ANY_LAT — The server first tries to resolve the name as a LAT service name. If that fails, the server then resolves it as a TELNET domain name. This is the default setting. ANY_TELNET — The server first tries to resolve the name as a TELNET domain name. If that fails, the server then resolve it as a LAT service name. LAT — The server should interpret the variable as a LAT service-name. Telnet — The server should interpret the variable as a Telnet domain-name or internet-address.
Idle Timeout	How many minutes before an inactive session will be disconnected. Possible values are from 0 to 255 (the default value is 0, which means that the session will not be disconnected for being inactive). Typically, the 0 setting is used to prevent "hanging printer" problems.
SLIP Address	The local *internet-address* assigned to the server port. You can map this address to a range of addresses by using the DEFINE PORT PPP SLIP MASK command.
Remote SLIP Addr	The *internet-address* assigned to a SLIP port. You can map this address to a range of addresses by using the DEFINE PORT PPP SLIP MASK command.

SHOW/LIST/MONITOR PORTS ALTERNATE CHARACTERISTICS (continued)

TCP Window Size — The size of the TCP window to be used when a TCP/IP session is started. the default value is 256.

DCD Timeout — The period of time, in milliseconds, that the DCD signal can be deasserted, before the software will disconnect the port. The default value is 2000.

Stop Bits — Shows the number which maps to the number of stop bits to be used to maintain synchronization of data. The following table indicates how many stop bits will be used for number shown in the display:

bit-value setting	**Stop Bits Used**
1	1 stop bit
2	2 stop bits
3	1.5 stop bits
4	The server calculates the number of stop bits to be used based on the port speed. This is the default and displays on a LIST screen. A SHOW or MONITOR display indicates the actual value in use.

TCP Keepalive Timer — Shows the number of minutes that the access server will wait for a response from the Telnet partner before terminating the session. Valid values are 0 - 30 minutes. The default is 0, which specifies no keepalive timer.

Nested Menu — The current setting of the Nested Menu feature. The valid values are: enabled, disabled, or enabled and required.

Command Size — The current size of the command input buffer. Valid values are: 80 to 16384 characters. The default setting is 80.

XDM Query — Displays only if XREMOTE is enabled on the server.

How the server locates an XDM manager.

SPECIFIC — Search for the host at the location in the *domain-name* or *internet-address* variable, which is the XDM manager.

BROADCAST — Search the network for an XDM manager using the Internet broadcast address.

INDIRECT — Search for the host at the location in the *domain-name* or *internet-address* variable. This host provides a list of XDM managers on the network.

SHOW/LIST/MONITOR PORTS ALTERNATE CHARACTERISTICS (continued)

XDM Host	Displays only if XREMOTE is enabled on the server. Shows the name of the XDM manager currently in use.
Rlogin Transparent Mode	If RLOGIN is enabled, characters are passed *raw* (without interpretation) and transparently within an RLOGIN session. This allows the ZMODEM transfer to complete.
Xon Send Timer	How many seconds between XON sends. The valid values are 0 through 2550 seconds. The default is 10 seconds. table
Slip Autosend	If enabled, SLIP addresses are automatically sent.
APD Prompt	If APD is enabled, the APD prompt will display on the Specified port. The default prompt is "".
DTR wait	Shows the conditions under which the port asserts the DTR modem control signal. The possible values are: Disabled, Enabled, FORCONNECTION, FORRING. The default setting is Disabled.
Typeahead size	Shows the size of the port type-ahead buffer (the number of bytes or characters that can be temporarily stored pending transmission). The default is 128.
SLIP Masks	Shows the *internet-subnet-mask* which is used by the server when determining whether to forward a packet over a SLIP link. The default is 255.255.255.255.
Default Session Mode	The mode to which all sessions are initially set. The possible values are: INTERACTIVE (the default), INTERACTIVE_NOIAC, LIMIT, PASSALL, PASTHRU, and TRANSPARENT.
Prompt	The local command prompt, which is displayed at the devices connected to the server serial port(s).
Dialback Timeout	If enabled, The amount of time that the remote modem (the modem being called) has to answer a dialback call.
Script Login	The current setting of the Script Login feature. Valid values are: Enabled, Disabled and Required. The default setting is Disabled.
Username Filtering	The current type of filtering (if any) used on the defined username. You can specify none or that the server only allow 7-bit printable characters.
Nested Menu Top Level	The current number of the highest-level menu for the ports you specify. The access server displays the highest-level menu first

SHOW/LIST/MONITOR PORTS ALTERNATE CHARACTERISTICS (continued)

Clear Security Entries	If enabled, one or all Internet security entries pertaining to the designated port(s) have been removed from the Internet Security table in the permanent database. Once cleared, a permanent database entry can be respecified using the DEFINE PORT IP SECURITY command. The server will display an error message if the entry you specify does not exist.
Login Duration	How many minutes a user can remain logged in to a port, regardless of the activity on the port. Valid values are: 0 (which indicates that this feature is disabled) or from 1 - 480 minutes.
TCP Outbound Address	The current unique source IP address for the port's outbound connection. The default is 0.0.0.0. If you use the default setting, the server's IP address is used as the source IP address, otherwise the source address is the TCP outbound address.
RADIUS Accounting	Shows the current status of RADIUS accounting. The valid values are: Enabled or disabled.
Username Prompt	Shows the username string assigned to this port. This is the prompt the user sees at login. When a user logs in to a port that has a username assigned, the port bypasses the Username prompt. (Depending on PASSWORD setting, the port may display a password prompt. If the PASSWORD is set to DISABLED, the port will display the Xyplex> prompt or connect to a dedicated service.) The username also appears in server displays.
Password Prompt	Displays the prompt users see at login to this port.

SHOW/LIST/MONITOR PORT ARAP CHARACTERISTICS Privilege: See Below

Use the SHOW/LIST/MONITOR SERVER ARAP display to view information about the settings that are currently specified for various ARAP characteristics at a port.

Privilege

Secure and non-privileged users can use LIST or SHOW PORTS commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORTS command.

Syntax

```
SHOW/LIST/MONITOR PORT [port-list] ARAP CHARACTERISTICS
                       [ALL]
```

Where	Means
port-list	One or more ports.
ALL	Display the requested information for all ports on the server.

Example

```
Xyplex> show port 1 arap characteristics

Port 1: SQA                                  09 Oct 1998  01:49:16

ARAP Enabled:               Enabled
ARAP Zone access:           All
ARAP Guest Logins:          Disabled
ARAP Maximum Connect Time:  0:60:00
Time Connected:             0:29:44
Time Remaining:             0:30:16
```

MONITOR/SHOW/LIST PORT ARAP CHARACTERISTICS

The following table describes the fields on the MONITOR/SHOW/ LIST PORT ARAP CHARACTERISTICS display:

Field	Description
Port *n*:	Shows the number of the port, *n*, and the username of the user who is logged on to the port.
ARAP Enabled:	Shows whether or not Remote Access is enabled at the port. Enabled means that the port is configured to support Remote Access connections. (In this case, other types of connections are not allowed.) Disabled means that the port is not configured to use Remote Access connections.

SHOW/LIST/MONITOR PORT ARAP CHARACTERISTICS (continued)

ARAP Zone access: Shows which, if any AppleTalk zones that are available to users at this port. If a specific zone-name is listed, the user only has access to that zone, in addition to the zone that the server is in. Otherwise, one of the following will be listed:

All	The user at this port has access to all AppleTalk zones.
Local	The user at this port has access only to the zone that the server is in.
None	The user at this port has access to no AppleTalk zones.

ARAP Guest Logins: Shows whether or not users at this port can log on to the device as a "guest" user (no password is required to log in as a guest user), rather than as a "registered" user. Enabled means that users can log on in as a guest user (or, optionally, as a registered user). Disabled means that the user must log on as a registered user. The default setting is disabled.

ARAP Maximum Connect Time: Shows the maximum amount of time (in minutes) that a user can remain connected to this port, if the port has been configured with a time limit. If there is no time limit, this field will show that the user can be connected for an "Unlimited" amount of time. When the ARAP session reaches the limit, the server will disconnect the session.

Time Connected: Shows the amount of time that the user in the current session has been connected to this port. (This field is only displayed in SHOW or MONITOR displays and only when ARAP is enabled at the port.)

Time Remaining: Shows the maximum amount of time (in minutes) that a user can remain connected to this port If there is no time limit for the currently connected session, this field will show that the user can be connected for an "Unlimited" amount of time. (This field is only displayed in SHOW or MONITOR displays and only when ARAP is enabled at the port.)

SHOW/MONITOR PORT ARAP COUNTERS Privilege: See Below

Use the SHOW/MONITOR PORT ARAP COUNTERS display to view information about the activity at ports which are configured to use Remote Access.

Counters in this display correspond to the interface counters in the SNMP MIB.

Privilege

Secure and non-privileged users can use LIST or SHOW PORTS commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORTS command.

Syntax

```
SHOW/MONITOR PORT [port-list] ARAP COUNTERS
                  [ALL]
```

Where	Means
port-list	One or more ports to be displayed.
ALL	Display the requested information for all ports on the server.

Example

```
Xyplex> show port arap counters

Port 1:                                    09 Oct 1998  19:51:53

Number of bytes received:                             0
Number of bytes transmitted:                          0
Number of uni-cast packets received:                  0
Number of uni-cast packets transmitted:               0
Number of received packets discarded:                 0
Number of transmitted packets discarded:              0
Number of received packets in error:                  0
Number of received packets of unknown type:           0
Length of transmit packet queue:                      0
```

MONITOR/SHOW PORT ARAP COUNTERS Display

The following table describes the fields on the MONITOR/SHOW PORT ARAP COUNTERS display:

SHOW/MONITOR PORT ARAP COUNTERS (continued)

Field	Description
Port *n*:	The number of the port, *n*, and the username of the user who is logged on to the port.
Number of bytes received:	The total number of bytes received by the serial port, since the counters were last reset to zero.
Number of bytes transmitted:	The total number of bytes sent by the serial port, since the counters were last reset to zero.
Number of uni-cast packets received:	The total number of ARAP unicast packets that have been received by the serial port, since the counters were last reset to zero.
Number of uni-cast packets transmitted:	The total number of ARAP unicast packets that have been transmitted by the serial port, since the counters were last reset to zero.
Number of received packets discarded:	The number of ARAP packets that have been received and discarded, since the counters were last reset to zero. A large value usually indicates poor telephone line quality or insufficient buffer (typeahead) capacity.
Number of transmitted packets discarded:	The number of ARAP packets that were not transmitted, since the counters were last set to zero.
Number of received packets in error:	The number of ARAP packets that have been received and discarded because they contained an error, since the counters were last reset to zero. A large value usually indicates poor telephone line quality.
Number of received packets of unknown type:	The number of packets that have been received and discarded because they did not appear to be ARAP packets, since the counters were last reset to zero. A large value could indicate poor telephone line quality.
Length of transmit packet queue:	The number of ARAP packets that have not yet been transmitted, since the counters were last reset to zero. A large value (greater than 3) means that the link is running slowly or that packets are being received from the Ethernet network too quickly to be processed.

SHOW/LIST/MONITOR PORT CHARACTERISTICS Privilege: See Below

Use these commands to view the current values for some basic port settings that have been defined by the user or the access server manager. The settings shown on this display are items related how data is transmitted by the port to the device (line speed, parity bit error checking, bits per character, flow and modem control, etc). This display is the "default" display shown when you issue a SHOW/LIST/MONITOR PORT command without specifying a port-list (i.e., for your own port) or any other keywords in the command.

Privileges

Secure and non-privileged users can use LIST or SHOW PORTS commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORTS command.

Syntax

```
SHOW/LIST/MONITOR PORT     [port-list]  CHARACTERISTICS
                           [ALL]
```

Where	Means
port-list	The port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.
ALL	Display the requested information about all ports.

Example

```
Xyplex>> show port characteristics


Port 1: DON1600                              17 Nov 1998  18:50:03

Character Size:            8          Input Speed:       19200
Flow Control:            XON          Output Speed:      19200
Parity:                 None          Modem Control:  Disabled
Access:                Local          Local Switch:       None
Backwards Switch:       None          Name:              PORT_4
Break:                 Local          Session Limit:          4
Break Length:          250ms          Type:                Soft
Forwards Switch:        None
CCL Modem Speaker: Inaudible          CCL Name:           None
APD Timeout:       Unlimited          APD Default:       LOGOUT
APD:                Disabled
Dialout Action:       Logout
APD Authentication
Interactive Only:   Disabled

Preferred Service: None

Authorized Groups: 0
(Current)  Groups: 0

Enabled Characteristics:
Autobaud,  Autoprompt,  Broadcast,  Input Flow Control,  Internet Connections,
Line Editor,  Loss Notification,  Message Codes,  OutboundSecurity,
Output Flow Control,  ULI,  Verification, Welcome Before Authentication
```

LIST/MONITOR/SHOW PORT CHARACTERISTICS Display

The following table describes the fields on the LIST/MONITOR/SHOW PORT CHARACTERISTICS display:

Field	Description
Port *n*	The number of the access server port, about which the system is displaying information. The variable *n* represents the number of a physical access server port.
user-name	The text which follows the port number shows either the name given by the user to log on to the port, or the name given to the port using SET/DEFINE PORT USERNAME.
Character Size	The number of bits per character for data characters that are transmitted or received over the serial connection between the access server port and the device connected to the port. The character size is either 7 or 8 bits. the default value is 8.

SHOW/LIST/MONITOR PORTS CHARACTERISTICS (continued)

Flow Control	The flow control ("handshaking") method used by the serial interface to control data transfer between the access server port and the device connected to the port. The possible values are: XON, CTS, DSR, XON_ALT, ENQ_HOST, ENQ_TERM, NONE (disabled). The default setting is XON.
Parity	The method by which the server and the device connected to the port check for single-bit errors in characters transmitted or received by the port. (This is called a parity check because the device provides an extra bit, called a parity bit, for error checking.) The possible values are: EVEN, NONE, and ODD. The default setting is NONE.
Access	The type of access the port can have to a service node, and/or the type of access other interactive users and service nodes can have to the port. The possible values are: Dynamic, Local, Remote or None. The default setting is Local.
Backwards Switch	The character that causes the access server to exit from the current session and connect to the next lower-numbered session, or NONE if this is undefined. Control characters are displayed as ^n (e.g., CTRL/B is shown as ^B). The default setting is NONE.
Break	The action the port will take when the user presses the BREAK key. The possible values are: Disabled, Local and Remote.

SHOW/LIST/MONITOR PORT CHARACTERISTICS (continued)

Break Length	Shows how long a break will be sent out the serial port in response to a TELNET BREAK. The valid values are: 250ms, 500ms, or 750ms. Note: This feature is not supported under LAT.
Forwards Switch	The character that causes the access server to exit from the current session and connect to the next higher-numbered session, or NONE if this is undefined. Control characters are displayed as ^n (e.g., CTRL/B is shown as ^B). The default setting is NONE.
CCL Modem Speaker	Shows if the CCL script is audible or inaudible while the modem establishes the connection. The default setting is INAUDIBLE.
APD Timeout	How much time the port will spend trying to determine which protocol is being used to make a connection. The valid timeout values are from 1 to 255 seconds or UNLIMITED (the port can continue indefinitely trying to determine which protocol is being used to make a connection). The default is UNLIMITED.
APD	If enabled, indicates that automatic protocol detection (APD) is enabled on the port.
Dialout Action	What action the port will take when the remote session made at a dialout port is terminated by the connection partner. The valid values are: PPP, SLIP, LOGOUT and Query. The default setting is LOGOUT.
APD Authenti-cation	Whether or not Interactive users will be prompted before or after the APD message displays and continue to use system-level authentication such as RADIUS or KERBEROS. The default setting is DISABLED, which means the server will prompt for authentication before the APD prompt is displayed.
Interactive Only	When this feature is enabled, users connecting with PPP or SLIP must use a protocol-level authentication (such as PAP or CHAP) or they will be able to connect without any authentication.
Input Speed	The rate, in bits per second, at which the device connected to the port receives data and the server port processes the data.
Output Speed	The rate, in bits per second, at which the server port transmits data and the device connected to the port processes the data.

Modem Control	If enabled, the device connected to the port uses modem control signals (e.g., uses DSRLOGOUT or DTRWAIT mode of operation). The possible values are: Disabled or Enabled. The default setting is Disabled. See the SET PORT MODEM CONTROL command for more information.
Local Switch	The character that causes the access server to exit from the current session and return to the local command mode, or None if this is undefined. Control characters are displayed as ^n (e.g., CTRL/B is shown as ^B). The default setting for Port 0 is the tilde (~). The remaining ports use NONE as the default.
Name	The server manager defined or default name of the port. The default setting is "Port_n" where *n* is the physical port number.
Session Limit	The maximum number of sessions that can simultaneously be connected by the port.
Type	How the attached device produces output, and how the server performs certain device specific functions, when the port is in local command mode. The possible values are: ANSI, SOFT and HARD. The default setting is SOFT.
CCL Name	If CCL Modem speaker is enabled, shows the name of the current CCL script.
APD Default	Displays what the APD default will be once connected. The valid values are: ARAP, SLIP, PPP, Interactive and Logout.
Preferred Service	The name of the LAT service or Telnet destination to which the port will be connected, whenever the user makes a connect request without specifying a *service-name.*. If the preferred service was defined with the CONTROLLED option, CONTROLLED appears in this field.
Authorized Groups	The *group-list* which includes the LAT services to which the server manager authorizes the port to have access (i.e., groups in the list represent services to which the port has access, groups not in the list represent services to which the port is denied access). The default setting is 0.
(Current) Groups	The *group-list* of LAT services to which the user has chosen to have access.The Current Groups list may be identical to or a subset of the Authorized Groups for the port.

Enabled Characteristics

The settings that have been enabled for the port using the DEFINE/SET PORT command.

By default only 12 of these possible values are enabled: AUTOBAUD, AUTOPROMPT, BROADCAST, INPUT FLOW CONTROL, INTERNET CONNECTIONS, LINE EDITOR, LOSS NOTIFICATION, MESSAGE CODES, OUTBOUNDSECURITY, OUTPUT FLOW CONTROL, ULI, and VERIFICATION.

Possible values are

Autobaud	indicates that the port determines the input port speed, parity, and character size for the device connected to the port, and automatically sets matching port characteristics.
Autoconnect	indicates that the port automatically connects to either a dedicated service or a preferred service when the user logs on to the port, or that the port will attempt to re-connect a session when a connection failure occurs.
Autodedicated	indicates that the unit will automatically log on the port and establish a connection to the dedicated service that is defined for the port when the unit is initialized or the port is logged out.
Autohangup	indicates the port will log out when the last session is terminated.
Autoprompt	indicates that the server will automatically prompt the LAT service node to run its login routine whenever a connection is made.
Broadcast	indicates that the port can receive messages that are broadcast from other ports on the unit.
Connectresume	indicates that the CONNECT command will resume an existing session with the specified destination, rather than establishing a new session to that destination.

Enabled Characteristics(continued)	
Dialback	indicates that the the port will attempt to dial back to a remote modem The port requires a dialback script in order to be logged in.
Dial Up	indicates that the port is considered to be connected to a dial-up line.
DSRlogout	The access server will log out the port when the serial interface DCD signal is deasserted.
DSRWait	The access server should begin the login sequence when the device asserts the DSR signal.
Interrupts	A local user (e.g., the user at the port) can interrupt a remote session at the port by entering the local switch character, or the <BREAK> character, if the PORT BREAK characteristic is set to LOCAL.
Inactivity	The server will log out the port after a specified period of Logout inactivity (specified by the SERVER INACTIVITY TIMER setting) has elapsed.
Input Flow Control	Flow control is used when data is transmitted by the connected device to the port.
Internet Connections	The port will be able to accept an *internet-address*, as well as addresses using the *domain-name* format to connect to a TCP/IP destination.
Kerberos	The port provides Kerberos user verification as part of the login process.
Limited View	Secure or non-privileged users cannot view SHOW/LIST DESTINATIONS, NODES, or SERVICES displays.
Line Editor	The command line editing feature is available at the port.

Loss Notification Indicates that the port sends a Bell character to the device connected to the port, whenever data input by the device is lost due to a receive data error or a data overrun error (e.g., make a terminal beep when the user types a command line that exceeds 132 characters.

Message Codes Indicates that the port displays the message code or number associated with a status or error message.

Menu indicates that a user at the port can only perform operations by choosing items from a menu that was defined by the server manager.

Noloss indicates that the port will store data in its typeahead buffer while waiting for a session connection to be made and then pass the data to the connection partner after the session connection is made.

Outboundsecurity If enabled, you can use Kerberos, SECURID, RADIUS or simple port password security features on port. The default setting is disabled.

Output Flow Control indicates that flow control is used when data is transmitted by the port to a device connected to the port.

Password indicates that a user must supply a local password in order to log on to the port.

Pause indicates the device attached to the port will show access server displays 24 lines at a time (by pausing at the end of 24 lines and waiting for the user to press a key before displaying the next 24 lines).

Privileged Menu indicates that the menu is enabled at the port, and the port is privileged.

PPP indicates that PPP is enabled for the port, and that the port expects all data to be received in PPP packets.

Queuing indicates that the port can place a received service connection request into a connection queue, when the requested LAT service is busy. This feature is not available for Telnet connections.

Radius	The port provides Radius user verification as part of the login process.
Remote Modification	indicates that certain PORT settings (of this port) can be changed by a process running at a VMS host.
Script Echo	indicates that the port will display the TCP/IP-LAT commands contained in a script file while they are being executed.
SecurID	The port provides SecurID user verification as part of the login process.
Security	indicates that the port is set to secure status (i.e., the user is restricted from using some port configuration commands and from viewing information about other ports or sessions, using the SHOW displays).
Signal Check	indicates that connections to a service offered at the port are disallowed when the DSR signal is deasserted or that when the DCD signal is deasserted, appropriately configured ports are logged out.
SLIP	Internet SLIP is enabled for the port. The port expects all data to be in SLIP packets.
ULI	If enabled, the UNIX-like interface is enabled on the server. This is the default.
Verification	The port displays informational messages whenever the user connects, disconnects, or switches a session.
Welcome Before Authentication	If enabled, the Xyplex Banner displays before any authentication prompt (i.e., Radius, SecurID, Kerberos). The default setting is disabled.

SHOW/MONITOR/LIST PORT CONTROLLED Privilege: S, N, P

Use these commands to display a list of controlled port strings. The strings are hexadecimal ASCII characters, enclosed in double quotes, with each byte separated by a space, such as "0d 0a"

The default string is the null string; a pair of double quotes(""). To clear a string, set it to the null string "".

Syntax

```
SHOW/MONITOR/LIST PORT [port-list]CONTROLLED
                       [ALL]
```

Example

```
Port 0:  access                              29 Sep 1998  13:44:25

Controlled Port Login: 1B 5B 48

Controlled Port Logout:

Controlled Session Inititialize: 07

Controlled Session Terminate:

MX1620>
```

SHOW PORT CONTROLLED

Field	Description
Controlled Port Login	If enabled, shows the string sent to the console during port login. The default string is a pair of double quotes (“ ”).
Controlled Port Logout	If enabled, shows the string sent to the console during port logout.
Controlled Session Initialize	The string to be sent to the console during a "CONNECT" controlled session.
Controlled Session Terminate	The string to be sent to the console during a "DISCONNECT" controlled session. The valid values are ASCII hexadecimal characters, from 0 to 32, enclosed in double quotes with each bytes separated by a space. The default string is the null string (a pair of double quotes""). To clear a string, set it to the null string "".

SHOW/MONITOR PORT COUNTERS — Privilege: See Below

Use the SHOW/MONITOR PORT display to view statistics about port activity.

Privileges

Secure and non-privileged users can use SHOW PORTS commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORT command.

Syntax

```
SHOW/MONITOR PORT    [port-list]    COUNTERS
                     [ALL]
```

Where	Means
port-list	Specifies the port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.
ALL	Display the requested information about all ports.

SHOW/MONITOR PORT Counters (continued)

Example

```
Xyplex>> show port counters


Port 1:  DON1600                              08 Oct 1998  08:40:21

Seconds Since Zeroed:         153792  Local Accesses:             2
Framing Errors:                    0  Remote Accesses:            0
Parity Errors:                     0  Idle Timeouts:              0
Overrun Errors:                    0
Input Count:                     842
Output Count:                  72874

SLIP Packets
 Serial Packets Received:        0  Network Packets Received:      0
 Serial Packets Sent:            0  Network Packets Sent:          0
 Serial Packets Discarded:       0  Network Packets Discarded:     0
 Serial Packet Length Errors:    0
 Serial Packet CheckSum Errors:  0
```

LIST/MONITOR/SHOW PORT COUNTERS Display

The following table describes each field on the LIST/MONITOR/SHOW PORT COUNTERS display

Field	Description
Port *n*	The access server's port number.
user-name	The name given by the user to log on to the port, or the name given to the port using the SET/DEFINE PORT USERNAME command.
Seconds Since Zeroed	The number of seconds since the counters were reset to zero.
Framing Errors	The number of bytes received at the port with illegally formatted frames (e.g., character garbled due to a missing stop bit), since the counter was reset to zero. Frequent framing errors (more than 20 per day for a terminal; 200 per day for a modem, due to line noise) may indicate a problem with the port or the device attached to the port, or mismatched settings (such as port speed, parity, character size, etc) between the port and the data received from the attached serial device connected to the port.

Parity Errors	The number of bytes received at the port with parity errors (e.g., a single bit error detected by a parity error check), since the counters were reset to zero. Frequent parity errors (more than 20 per day for a terminal; 200 per day for a modem, due to line noise) may indicate a problem with the port or the device attached to the port, or mismatched settings (such as port speed, parity, character size, etc) between the port and the device connected to the port.
Overrun Errors	The number of times characters were lost because the access server input buffers were full, since the counters were reset to zero. Overrun errors indicate that there may be a flow control problem, such as mismatched flow control methods, between the port and the device connected to the port.
Input Count	The number of characters (bytes) transmitted to the port by the device connected to the port, since the counters were reset to zero.
Output Count	The number of characters (bytes) transmitted by the port to the device connected to the port, since the counters were reset to zero.
Local Accesses	The number of times a user has logged on to the port from a local device attached to the port, since the counters were reset to zero.
Remote Accesses	The number of times a remote-access connection (e.g., from a remote node across the LAN) was established on the port, since the counters were reset to zero.
Idle Timeouts	The number of times that the access server has disconnected a session, that was initiated by the remote connection queue, for being inactive, since the counters were reset to zero.

SHOW/MONITOR PORT COUNTERS (continued)

NOTE: *The following fields only display when SLIP is enabled on the port.*

Serial Packets Received	The number of SLIP packets received from the remote device.
Serial Packets Sent	The number of SLIP packets sent by the port to the remote device.
Serial Packets Discarded	The number of SLIP packets that have been discarded by the server.
Serial Packet Length Errors	The number of SLIP packets received by the port that did not contain the correct number of bytes.
Serial Packet Checksum Errors	The number of SLIP packets received by the port that contained incorrectly transmitted data
Network Packets Received	The number of Ethernet packets received by the server that have been converted to SLIP packets.
Network Packets Sent	The number of Ethernet packets sent by the server that have been converted from SLIP packets.
Network Packets Discarded	The number of Ethernet packets that have been discarded by the server.

SHOW/LIST/MONITOR PORT IP SECURITY Privileges: See Below

Use these commands to view the entries in the IP Security table. See the Security Features chapter in the *Advanced Configuration Guide* for a description of the IP Security feature.

Privileges

Secure and non-privileged users can use LIST or SHOW PORTS commands (secure users can only display information about the port they are logged on to). Only users at privileged . can use the MONITOR PORTS command.

Syntax

```
SHOW/LIST/MONITOR PORTS  [port-list] INTERNET SECURITY [INBOUND]   [ALLOW]
                         [ALL]                         [DENY]
                                                       [OUTBOUND]  [ALLOW]
                                                                   [DENY]
                                                       [internet-address]

                         [ACCESS]  [DYNAMIC]
                                   [LOCAL]
                                   [REMOTE]
                                   [NONE]
```

Where	Means
port-list	Specify the port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.
ALL	The requested information about all ports.
ACCESS	The requested information about all ports that have an access setting: of dynamic, local, remote or none See the DEFINE/SET PORT ACCESS command description.
DYNAMIC	The requested information about all dynamic ports.
LOCAL	The requested information about all local ports.
REMOTE	The requested information about all remote ports.
NONE	The requested information about all ports that do not have access (set to NONE).

INBOUND	View inbound entries. If you do not specify the direction, inbound and outbound entries will both be listed.
OUTBOUND	View outbound entries. If you do not specify the direction, inbound and outbound entries will both be listed.
ALLOW	View entries for which inbound or outbound connections are permitted.
DENY	View entries for which inbound or outbound connections are not permitted.
internet-address	A variable -- if you enter an Internet address, the access server will inform you whether a connection to the address (outbound) or from the address (inbound) is possible for the specified port.

Example

```
Xyplex>> SHOW PORT 1 IP SECURITY

Inbound Default:  Allowed      Outbound Default:  Allowed

                 Internet           Security
Entry            Address             Mask            Access         Direction

 1              192.12.119.206    255.255.0.0         Allow          Outbound
 2              192.13.119.45     255.255.255.0       Allow          Inbound
 3              192.11.110.40     255.255.255.255     Deny           Outbound
```

SHOW/LIST PORT IP SECURITY DISPLAY

The following list describes each field on the LIST/MONITOR/SHOW PORT IP SECURITY display

Field	Description
Inbound Default	Shows whether inbound connections are allowed or denied by default.
Outbound Default	Shows whether outbound connections are allowed or denied by default.
Entry	The number of the entry in the port's Internet Security table.
Internet Address	The target address of the destination.
Security Mask	Describes how to interpret the target address.
Access	Either Deny (prevent connection) or Allow (permit connection).
Direction	Either Inbound (from the network) or outbound (to the network).

SHOW/LIST/MONITOR PORT KEYMAP Privilege: See Below

Use the SHOW/LIST/MONITOR PORT KEYMAP display to view TN3270 keymap listings.

Privileges

Secure and non-privileged users can use LIST or SHOW PORT commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORTS command.

Syntax

```
SHOW/LIST/MONITOR PORTS [port-list] KEYMAP
                        [ALL]
```

Where	Means
port-list	Specifies the port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.
ALL	The requested information about all ports.

Example

```
Xyplex> SHOW PORT 1 KEYMAP
Address:   08-00-87-00-4F-A4   Name:   X004FA4                Number:    0

Device: VT100       TerminalType: VT100                  Tn3278Type : MODEL2

Keymap:    3270-Key             KeyCode                      Description

           NEWLINE          :   "0A"                         "LF   "
           TAB              :   "09"                         "TAB  "
           BACKTAB          :   "1B 09"                      "ESCTB"
           CURSORUP         :   "1B 5B 41"                   "KEYUP"
           CURSORLEFT       :   "1B 5B 44"                   "KEYBK"
           CURSORRIGHT      :   "1B 5B 43"                   "KEYFW"
           CURSORDOWN       :   "1B 5B 42"                   "KEYDN"
           HOME             :   "1B 68"                      "ESCh "
           DELETE           :   "7F"                         "DEL  "
           ERASEEOF         :   "05"                         "CTRLe"
           ERASEINPUT       :   "1B 69"                      "ESCi "
           INSERT           :   "1B 7F"                      "ESCDL"
           FLUSHINPUT       :   "1B 66"                      "ESCf "
           REFRESH          :   "1B 72"                      "ESCr "
           CENTSIGN         :   "1B 63"                      "ESCc "
           DUPLICATE        :   "04"                         "CTRLd"
           FIELDMARK        :   "06"                         "CTRLf"
           SCROLL           :   "1B 6C"                      "ESCl "
           STATUS ON/OFF    :   "1B 3F"                      "ESC? "
           RESET            :   "12"                         "CTRLr"
           FASTLEFT         :   "16"                         "CTRLv"
           FASTRIGHT        :   "15"                         "CTRLu"
           SHOWKEYS         :   "18"                         "CTRLx"
           PRINT            :   "10"                         "CTRLp"
           PF1              :   "1B 4F 71"                   "NUM 1"
```

```
        PF2             :   "1B 4F 72"              "NUM 2"
        PF3             :   "1B 4F 73"              "NUM 3"
        PF4             :   "1B 4F 74"              "NUM 4"
        PF5             :   "1B 4F 75"              "NUM 5"
        PF6             :   "1B 4F 76"              "NUM 6"
        PF7             :   "1B 4F 77"              "NUM 7"
        PF8             :   "1B 4F 78"              "NUM 8"
        PF9             :   "1B 4F 79"              "NUM 9"
        PF10            :   "1B 4F 50"              "PF1  "
        PF11            :   "1B 4F 51"              "PF2  "
        PF12            :   "1B 4F 52"              "PF3  "
        PF13            :   "1B 21"                 "ESC! "
        PF14            :   "1B 40"                 "ESC@ "
        PF15            :   "1B 23"                 "ESC# "
        PF16            :   "1B 24"                 "ESC$ "
        PF17            :   "1B 25"                 "ESC% "
        PF18            :   "1B 5E"                 "ESC^ "
        PF19            :   "1B 26"                 "ESC& "
        PF20            :   "1B 2A"                 "ESC* "
        PF21            :   "1B 28"                 "ESC( "
        PF22            :   "1B 29"                 "ESC) "
        PF23            :   "1B 5F"                 "ESC_ "
        PF24            :   "1B 2B"                 "ESC+ "
        PA1             :   "1B 2C"                 "ESC, "
        PA2             :   "1B 2E"                 "ESC. "
        PA3             :   "1B 2F"                 "ESC/ "
        SYSREQ          :   "1B 73"                 "ESCs "
        ENTER           :   "0D"                    "ENTER"
        CLEAR           :   "03"                    "CTRLc"
        CURSORSEL       :   "1B 6B"                 "ESCk "
        TEST            :   "1B 74"                 "ESCt "
```

SHOW PORT KEYMAP DISPLAY

Field	Description
Device	The name of the TN3270 device in the display.
TerminalType	The local terminal type.
Tn3278Type	The model of TN3270 device that the local terminal terminal emulates during a TN3270 session.
Keymap	The table that follows contains the escape sequences that the access server uses to translate entries on the local ASCII keyboard into 3270 display station functions.
3270-Key	An IBM display station function.
KeyCode	The hexadecimal value for the keyboard escape sequence at the local terminal which corresponds to the IBM display station function.
Description	A text description of the keyboard function.

SHOW/LIST/MONITOR PORT PPP CHARACTERISTICS Privilege: N, P

Use the SHOW/LIST/MONITOR PORT PPP CHARACTERISTICS commands to display PPP characteristics that will be negotiated by the access server on one or more ports.

Syntax

```
SHOW/LIST/MONITOR PORT [port-list] PPP CHARACTERISTICS
                       [ALL]
```

Where	Means
port-list	One or more access server ports.
ALL	Display the requested information for all ports on the server.

Example

```
Port 6:                                  08 Oct 1998  14:02:46
PPP Characteristics

Protocol(s):  IP, IPX

Active:                             Enabled
PAP Authentication:                    None
CHAP Authentication:                   None
CHAP Challenge Timer (min):               0

Charmap:                         0x000a0000
MRU:                                   1500
Restart Timer:                            3
Failure Limit:                            3
Configure Limit:                         10

Logging:                               None
Keepalive Timeout:                        6
Keepalive Timer:                          6
Magic Number:                       Enabled

MX1620>>
```

SHOW/LIST/MONITOR PORT PPP CHARACTERISTICS Display

SHOW/LIST/MONITOR PORT PPP CHARACTERISTICS (continued)

Field	Description
Port *x*	The port number being displayed.
Active	Enabled means that the access server port can initiate the negotiation of PPP options. Disabled means that the port will wait until the remote device initiates the negotiation of PPP options.
PAP Authentication	If enabled, the remote device must supply the login password in order to establish a PPP connection with the port. Valid values are: Enabled, Disabled, Kerberos and Radius.
CHAP Authentication	If enabled, the remote device must supply the login password. Valid values are: Enabled, Disabled, and Radius.
CHAP Challenge Timer	Displays how many seconds the server will wait before re-challenging a peer after connection. A value of “0” disables this feature.
Charmap	The character-mask consisting of eight hexadecimal characters that represents which ASCII control character options the link will encode prior to transmission or decode upon receipt.
MRU	(Maximum Receive Unit). The maximum number of bytes of data and overhead that can be transmitted in a single frame over the PPP link. This number is fixed at 1500.
Restart Timer	How many seconds the port waits before sending another option configuration request packet. The value is 1 to 10 seconds, with a default setting of 3 seconds.
Failure Limit	The maximum number of times the port will object to unacceptable value for a PPP option, before the port rejects further negotiation of the option. The default setting is 3 times.
Configure Limit	The maximum number of unanswered PPP option configuration request packets that the port will send, before the software concludes that the remote device is unable to respond. When the port has reached this limit, it discontinues further attempts to negotiate PPP options and goes into a passive "listening" state. The default setting is 10 unanswered request packets.

SHOW/LIST/MONITOR PORT PPP CHARACTERISTICS (continued)

Logging	If enabled, how status or debug information PPP packets will be logged in the accounting log. INTERPRETED interprets the PPP packets in the accounting log. RAW logs the raw packets in Hex to the accounting log. NONE no packets are logged in accounting log.
Keepalive Timeout	If enabled, displays how many seconds the PPP link will wait for an LCP echo reply before closing the link. Use this feature to provide a keepalive between the port and the attached devices. Valid values are 0 - 65535 seconds. The default is 6 seconds.
Keepalive Timer	Specifies how many seconds the server will wait for an LCP echo request. The server will transmit a null message over a LAT virtual circuit, when there is no other traffic originating at the server. Valid values are between 10 and 180 seconds. The default value is 20 seconds
Magic Number	If enabled, helps to detect links that are in loopback condition. The default is enabled.

SHOW/MONITOR PORT PPP COUNTERS Privilege: N, P

Use these commands to display statistics about PPP activity at a port.

Syntax

```
SHOW/MONITOR PORT [port-list] PPP COUNTERS
                  [ALL]
```

Where	Means
port-list	One or more access server ports.
ALL	Display the requested information for all ports on the server.

Example

```
Xyplex>> show port 4 ppp counters


Port 4:                                  08 Dec 1998  08:43:53
LCP/HDLC Counters                   Received      Transmitted

LCP Config Req:                            0                0
LCP Config Nak:                            0                0
LCP Config Ack:                            0                0
LCP Config Rej:                            0                0
LCP Term Req:                              0                0
LCP Term Ack:                              0                0
LCP Echo Req:                              0                0
LCP Echo Reply:                            0                0
LCP Code Reject:                           0                0
LCP Protocol Reject:                       0                0
HDLC Total Packets:                        0                0
HDLC Framing Errors:                       0                -
HDLC Packet Bad Checksum:                  0                -
HDLC No Packet Errors:                     0                0
HDLC Discards:                             0                0
```

SHOW/MONITOR PORT PPP COUNTERS Display

Note: *The numbers displayed on this screen are based on the number of packets transmitted or received since the port counter was last reset to zero.*

Field	Description
LCP Config Req:	The number of Link Control Protocol (LCP) packets transmitted or received containing proposed option negotiation parameters.
LCP Config Nak:	The number of LCP packets transmitted or received containing option negotiation counter-proposals.

SHOW/MONITOR PORT PPP COUNTERS (continued)

LCP Config Ack:	The number of LCP packets transmitted or received acknowledging acceptance of proposed option values.
LCP Config Rej:	The number of LCP packets transmitted or received rejecting negotiation of the proposed option.
LCP Term Req:	The number of LCP packets transmitted or received containing requests to terminate the link.
LCP Term Ack:	The number of LCP packets transmitted or received containing acknowledgement that the link will be terminated.
LCP Echo Req:	The number of LCP packets transmitted or received which test the ability of the remote device to transmit and receive packets.
LCP Echo Reply:	The number of LCP packets transmitted or received in reply to an LCP Echo Request packet.
LCP Code Reject:	The number of LCP packets transmitted or received in response to receipt of an unrecognizable LCP packet.
LCP Protocol Reject:	The number of LCP packets transmitted or received indicating that the peer attempted to negotiate or use an unsupported protocol.
HDLC Total Packets:	The total number of Asynchronous High-Level Data Link Control (HDLC) frames transmitted or received on the link. Asynchronous HDLC is the framing technique used on PPP links.
HDLC Framing Errors:	The number of packets received which were framed incorrectly.
HDLC Packet Bad Checksum:	The number of packets received which contained an incorrect checksum.
HDLC No Packet Errors:	The number of packets transmitted or received which were discarded due to insufficient resources.
HDLC Discards:	Rx - The number of broadcast packets received that were discarded for any other reason (than those listed above).
:	Tx - The number of broadcast packets that were attempted to be transmitted out the port, but could not because the PPP QUEUE LIMIT has been reached. This counter can only be incremented when PPP IP BROADCAST is enabled on the port in question.

SHOW/MONITOR PORT PPP IP CHARACTERISTICS Privilege: N, P

Use these commands to display PPP IP settings that will be negotiated by the access server on one or more ports.

Syntax

```
SHOW/MONITOR PORT [port-list] PPP CHARACTERISTICS
                  [ALL]
```

Where	Means
port-list	One or more access server ports.
ALL	Display the requested information for all ports on the server.

Example

```
Xyplex>> show port 2 ppp internet char

Port 2:                                  08 Oct 1998  08:45:35
PPP IP Characteristics:

Local IP Address:             0.0.0.0
Local IP Range:               0.0.0.0 - 255.255.255.255
Remote IP Address:            0.0.0.0
Remote IP Range:              0.0.0.0 - 255.255.255.255
IP Broadcast:                Disabled
IP Mask:             255.255.255.255
VJ Compression:               Enabled
VJ Slots:                           3
```

SHOW/MONITOR PORT PPP IP CHARACTERISTICS Display

SHOW/MONITOR PORT PPP IP CHARACTERISTICS (continued)

Field	Description
Local IP Address	The Internet address assigned to the port.
Local IP Range	Display the currently assigned range of local IP addresses. Valid values that the port can negotiate are 0.0.0.0 - 255.255.255.255.
Remote IP Address	The IP address of the remote device that the port will attempt to negotiate when the remote device does not specify an Internet address on its own.
Remote IP Range	Display the currently assigned range of remote IP addresses. Valid values that the port can negotiate are 0.0.0.0 - 255.255.255.255.
IP Broadcast	Shows whether or not IP broadcast packets can be transmitted over the PPP link, or whether or not the port will forward broadcast packets received from the remote device to the local area network.
IP Mask	Specifies the range of IP addresses to mapped to the port. The valid range for an IP MASK is 0.0.0.0 - 255.255.255.255. The default setting is 255.255.255.255 to prevent ARPing on the link.
VJ Compression	Shows whether or not the port is allowed to negotiate the use of Van Jacobson compression. If enabled, the port is allowed to negotiate the use of Van Jacobson compression. If disabled, the port cannot use Van Jacobson compression. The default setting is Enabled.
VJ Slots	Shows the number of sessions (or slots) using Van Jacobson compression operating across the link that the port will attempt to negotiate. The default setting is 3.

SHOW/MONITOR PORT PPP IP COUNTERS Privilege: N, P

Use these commands to display statistics about PPP IP activity at a port that will be negotiated by the access serve.

Syntax

```
SHOW/MONITOR PORT [port-list] PPP IP COUNTERS
                  [ALL]
```

Where	Means
port-list	One or more access server ports.
ALL	Display the requested information for all ports on the server.

Example

```
Xyplex>> show port 2 ppp internet counters

Port 2:                                  08 Oct 1998  08:45:59
IPCP Counters                 Received         Transmitted

IPCP Config Req:                     0                   0
IPCP Config Nak:                     0                   0
IPCP Config Ack:                     0                   0
IPCP Config Rej:                     0                   0
IPCP Term Req:                       0                   0
IPCP Term Ack:                       0                   0
IP Total Packets:                    0                   0
```

SHOW/MONITOR PORT PPP IP COUNTERS Display

Note: *The numbers displayed on this screen are based on the number of packets transmitted or received since the port counter was last reset to zero.*

Field	Description
IPCP Config Req:	The number of Internet Protocol Control Protocol (IPCP) packets transmitted or received containing proposed option negotiation parameters.
IPCP Config Nak:	The number of IPCP packets transmitted or received containing option negotiation counter-proposals.
IPCP Config Ack:	The number of IPCP packets transmitted or received acknowledging acceptance of proposed option values.
IPCP Config Rej:	The number of IPCP packets transmitted or received rejecting negotiation of the proposed option.
IPCP Term Req:	The number of IPCP packets transmitted or received containing requests to terminate the link.
IPCP Term Ack:	The number of IPCP packets transmitted or received containing acknowledgement that the link will be terminated.
IP Total Packets:	The total number of IP datagrams transmitted or received on the link.

SHOW/MONITOR PORT PPP IP STATUS Privilege: N, P

Use these commands to display the PPP IP characteristics that have been negotiated by the access server on one or more ports.

Syntax

```
SHOW/MONITOR PORT [port-list] IP STATUS
                  [ALL]
```

Where	Means
port-list	One or more access server ports.
ALL	Display the requested information for all ports on the server.

Example

```
Xyplex>> show port 2 ppp ip status


Port 2:                                  08 Oct 1998  08:46:32
IPCP State:   OPEN

                        Local                Remote
IP Addresses:           142.179.248.146  140.179.248.148
VJ Compression:         Disabled                    -
VJ Slots:                      3                   15
```

SHOW/MONITOR PORT PPP IP STATUS Display

Where	Means
IPCP State	A system-defined field that lists the current IPCP state.
IP Addresses	The Internet address currently used on the link of the port (Local) and of the remote device (Remote).
VJ Compression	If enabled, the port can use VJ compression. If disabled, cannot use VJ compression.
VJ Slots	The number of sessions (or slots) using VJ compression operating across the link.

SHOW/MONITOR PORT PPP STATUS Privilege: N, P

Use these commands to display the PPP settings that have been negotiated by the access server on one or more ports.

Syntax

```
SHOW/MONITOR PORT [port-list] PPP STATUS
                  [ALL]
```

Where	Means
port-list	One or more access server ports.
ALL	Display the requested information for all ports on the server.

Example

```
Xyplex>> show port 2 ppp status

Port 2:                                  08 Oct 1998  08:48:12

LCP Status:   NONE

LCP Option                     Local        Remote
Charmap:                       N/A          N/A
Protocol Comp:                  N/A          N/A
Address Comp:                   N/A          N/A
Logging:                     Enabled      Enabled
Magic Number:                 Enabled      Enabled
```

SHOW/MONITOR PORT PPP STATUS Display

Field	Description
LCP Status	A system-defined field that gets filled in based on the current LCP state.
Charmap	The HDLC character encoding currently in use for each direction of the link.
Protocol Comp	If enabled, protocol field compression is in use for each direction of the link.
Address Comp	If enabled, address and control field compression is in use for each direction of the link.
Logging	If enabled, controls whether messages are sent to the accounting log. The default setting is Disabled.
Magic Number	If enabled, the magic number feature detects loops in the PPP link. If disabled, no loop detection is performed. The default setting is Enabled.

SHOW/LIST PORT SCREENMAP Privilege: N, P

Use these commands to view information about the TN3270 device enabled at the port.

Syntax

```
SHOW/LIST PORT [port-list]  SCREENMAP
               [ALL]
```

Where	Means
port-list	One or more access server ports.
ALL	Display the requested information for all ports on the server.

Example

```
Xyplex>> SHOW PORT 1 SCREENMAP
Port 1: DON1600                          09Jul 1998  08:23:44
Screenmap: Terminal Function    HexCode

           EraseEOL          :   "1B 5B 4B"
           ClearScr          :   "1B 5B 32 4A"
           MoveCursor        :   "1B 5B F8 3B FA 48"
           Col132            :   "1B 5B 3F 33 68"
           Col80             :   "1B 5B 3F 33 6C"
           Beep              :   "07"
           BoldOn            :   "1B 5B 30 3B 31 6D"
           BoldOff           :   "1B 5B 30 6D"
           Reset1            :   "1B 5B 3F 38 3B 32 68 1B 3D 1B 5B 30 71"
           Reset2            :   "1B 5B 3F 33 3B 37 3B 31 6C 1B 5B 48"
           Reset3            :   "1B 5B 32 4A 1B 5B 34 69"
           MoveCursor Base   :   1
           SGR               :   Enabled
```

SHOW/LIST PORT SCREENMAP Display

The display shows the escape sequences that the access server sends to the local terminal in order to initiate screen functions such as clear the screen, move the cursor, or set the bold attribute.

Terminal Function	The IBM screen function that occurs on the local terminal when the user enters the escape sequence indicated by the corresponding Hex Code.
Hex Code	The hexadecimal value of the escape sequence for the IBM terminal function.

SHOW/MONITOR PORT STATUS — Privilege: See Below

Use these commands to view detailed information about the current session to which the port is connected.

Privilege

Secure and non-privileged users can use SHOW PORT commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORT command.

Syntax

```
SHOW/MONITOR PORT    [port-list] STATUS
                     [ALL]
```

Where	Means
port-list	Specifies the port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.
ALL	Display the requested information for all ports on the server.

SHOW/MONITOR PORT STATUS (continued)

Example of a LAT Session

```
Xyplex>> SHOW PORT 1 STATUS
Port  1:  aa                            Server:                 X03346B

Access:                     Local       Current Service:          VMSHOST
Status:                 Connected       Current Node:
Sessions:                       0       Current Port:

Input XOFFed:                  No       Output Signals:         DTR, RTS
Output XOFFed:                 No       Input Signals:              DSR

Last Char Output:              20       Last Char Input:             0d
Script Host:

Script File:
```

Example of a Telnet Session

```
Xyplex> SHOW PORT 1 STATUS

 Port 1:  J. Smith                     Server:               X002771

 Access:                Local          Current Service:       TELNET
 Status:            Connected          Current Node:   192.12.119.128
 Sessions: 1                           Current Port:              23
 Current Domain:                               FINANCESUN.XYPLEX.COM

 Input XOFFed:              No         Output Signals:          None
 Output XOFFed:             No         Input Signals:           None

 Last Char Output:          74         Last Char Input:           0d

 Script Host:       192.12.119.8    unixhost

 Script File   /tftpboot/JSmith/login
```

Parallel Printer Port session

```
Port  3:  (Remote)                    Server:               X0085D4

 Access:                   Remote     Current Service:       TELNET
 Status:                Connected     Current Node:   192.12.119.128
 Sessions:                      1     Current Port:              23
 Current Domain:                               FINANCESUN.XYPLEX.COM

 Last Char Output:             6a     Last Char Input:          N/A

 Printer Interface:     Centronics
 Printer Fault:                No     Printer Busy:             Yes
 Printer Online:              Yes     Printer Paper:            Out
```

LIST/MONITOR/SHOW PORT STATUS Display

SHOW/MONITOR PORT STATUS (continued)

The following table describes each field on the LIST/MONITOR/SHOW PORT STATUS display.

Field	Description
Port *n*	The port number about which the system is displaying information. The variable *n* represents the number of a physical access server port.
user-name	The text which follows the port number shows either the name given by the user to log on to the port, or the name given to the port using the SET/DEFINE PORT USERNAME command.
Server	The name of the server unit.
Access	The type of connections the server allows to the port (e.g., the type of access the port can have to a service node, and/or the type of access other interactive users and service nodes can have to the port). The possible values are: Local, Remote, Dynamic, and None.
Status	The current status of the port. The possible values are:
Autobaud	The port is being autobauded.
Available	A port, that is set to REMOTE or DYNAMIC, is not busy.
Check Modem	The port is verifying that modem signals are properly asserted.
Check Connect	The port is determining the status (accepted or rejected) of a pending connection.
Connected	The port is currently connected to a LAT service or Telnet destination.
Connect Wait	The port is waiting to retry a connection attempt (used when PORT AUTOCONNECT is set to ENABLED).
Connecting	The port is currently attempting to connect to a LAT service or Telnet destination.
Dialback Wait	The Port is waiting for the remote modem to answer a dial-back call.

Disconnected	Shows that a session was disconnected (for example, for being inactive for too long).
Disconnecting	Shows that a session is disconnecting from a LAT service or Telnet destination.
Executing Cmd	The port is executing a command from the access server local command mode.
Finding Script	The port is searching for a script file via TFTP read requests.
First Dialback Login	The port is making its first attempt to locate a dial-back script.
Idle	The port is not in use.
Loading Script	The port has located a script file and is receiving the file from the script server.
Local Mode	The port is logged on to the server, and is in the local command mode.
Locked	The user has used the LOCK command to disable the port.
Login	The port is waiting for the user to enter a login or Kerberos password.
Login Wait	The port has been disabled (for 60 seconds) because an incorrect password has been entered, or because a dial-back attempt has failed.
Logout	The port is being logged out.
Password	The port is waiting for the user/application to enter the password that is required by a password-protected port.
PPP	The port is a PPP port.
Reset	The port is reverting to its stored configuration.
Retry Connect	The port is trying to connect to a service that was previously unavailable (used when PORT AUTOCONNECT is set to ENABLED).
Running Script	The port is executing the commands contained in a script file.

Second Dialback Login	The port is making its second attempt to locate a dial-back script (the port searches the directory path "above" the path specified for this script server).
Slip	The port is a SLIP port.
Suspended	The user has entered the local-switch character, and the session is being suspended.
Test Wait	The port is performing a TEST SERVICE command.
Test Out	The port is outputting the results of a TEST SERVICE command.
Wait Input	The port is at the local prompt (waiting for the user to enter a command).
Wait Logout	The port is waiting for modem control signals to be deasserted.
Wait Output	The port is completing display output before logging out.
Wait Queue	A connection request from this port is in a queue.
Wait Session	The session is being disconnected.

Sessions	The number of active sessions on the port.
Current Domain	Only displayed when the user is in a Telnet session. Shows the domain-name or internet-address to which the port is connected.
Current Service	The currently active service session, or the service session that was interrupted when the user entered local mode. If the user is in a Telnet session, the word TELNET will be displayed.
Current Node	The name of the LAT service node, or the internet-address of the Telnet node, to which the current session is connected. For remote connections to local services, this shows the name or internet-address of the node from which the connection originated.
Current Port	The identification of the port at the service node or at the requesting node. If the user is in a Telnet session, shows the telnet-port number.

Input XOFFed	Shows whether or not XON/XOFF flow control is enabled for data input to the port from the device connected to the port.
Output XOFFed	Shows whether or not XON/XOFF flow control is enabled for data output from the port to the device connected to the port.
Output Signals	Shows modem control signals that are currently asserted by the port to the device connected to the port. This field is not shown for parallel ports.
Input Signals	Shows modem control signals that are monitored by the port (asserted by the device connected to the port. This field is not shown for parallel ports.
Last Char Output	The hexadecimal value of the last character sent by the port to the device attached to the port.
Last Char Input	The hexadecimal value of the last character received by the port from the device attached to the port.
Script Host	The internet-address/domain-name of the script server where the port obtained a script file to run.
Script File	The name of the script file that was obtained from the host shown in the "Script Host" field.

Parallel Printer Information (MX 1400 and MX 1450 only)

Printer Interface	The type of parallel printer interface used. The possible values are Centronics or Dataproducts.
Printer Fault	Indicates whether or not the parallel printer is reporting a printer fault. The possible values are Yes and No.
Printer Online	Indicates whether or not the parallel printer is currently online (available for printing). The possible values are Yes and No.

Printer Busy	Indicates whether or not the parallel printer is currently printing. The possible values are Yes and No.
Printer Paper	Indicates whether or not the parallel printer is reporting that it has paper. The possible values are Yes and Out. Note: This field does not display for the MAXserver 1400 Printer when a Dataproducts interface is used.

SHOW/LIST/MONITOR PORT SUMMARY Privilege: See Below

Use the SHOW/LIST/MONITOR PORTS SUMMARY display to view a one-line summary showing the access method, connection status, and services in use at the specified port(s). This display is the "default" display shown when you issue a SHOW/LIST/MONITOR PORT command and you include a port-list (i.e., to display information about multiple ports or all ports) in the command.

Privilege

Secure and non-privileged users can use SHOW PORT commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORT command.

Syntax

```
SHOW/LIST/MONITOR PORTS    [port-list]   SUMMARY
                           [ALL]
```

Where	Means
port-list	The port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.
ALL	The requested information for all ports on the server.

Example

```
Xyplex>> show ports all summary

Port    Access    Status        Services Offered        08 Oct 1998  08:51:57

  1     Local     Wait Input
  2     Local     Idle
  3     Local     Idle
  4     Local     Idle
  5     Local     Idle
  6     Local     Idle
  7     Local     Idle
  8     Local     Idle
  9     Remote    Connecting          LASER
 10     Local     Idle
 11     Local     Idle
 12     Local     Idle
 13     Local     Idle
 14     Local     Idle
 15     Local     Idle
 16     Local     Idle
 17     Local     Idle
 18     Local     Idle
 19     Local     Idle
 20     Local     Idle
```

LIST/MONITOR/SHOW PORT SUMMARY Display

The following table describes each field on the LIST/MONITOR/SHOW PORT SUMMARY display PORT

Field	Description
Port	The number of the access server port, about which the system is displaying information.
Access	The type of connections which the access server allows to the port (e.g., the type of access the port can have to a service node, and/or the type of access other interactive users and service nodes can have to the port). The possible values are LOCAL, DYNAMIC, REMOTE and NONE.
Status	The current status of the port. The possible values are:
Autobaud	The port is being autobauded.
Available	A port that is set to REMOTE or DYNAMIC, is not busy.
Check Modem	The port is verifying that modem signals are properly asserted.
Check Connect	The port is determining the status (accepted or rejected) of a pending connection.

Connected	The port is currently connected to a LAT service or Telnet destination. PORT
Connect Wait	The port is waiting to retry a connection attempt (used when PORT AUTOCONNECT is set to ENABLED).
Connecting	The port is currently attempting to connect to a LAT service or Telnet destination.
Dialback Wait	The Port is waiting for the remote modem to answer a dial-back call.
Disconnected	Shows that a session was disconnected (for example, for being inactive for too long).
Disconnecting	Shows that a session is disconnecting from a LAT service or Telnet destination.
Executing Cmd	The port is executing a command from the access server local command mode.
Finding Script	The port is searching for a script file via TFTP read requests.
First Dialback Login	The port is making its first attempt to locate a dial-back script.
Idle	Shows that the port is not in use.
Loading Script	The port has located a script file and is receiving the file from the script server.
Local Mode	The port is logged on to the server, and is in the local command mode.
Locked	The user has used the LOCK command to disable the port.
Login	The port is waiting for the user to enter a login or Kerberos password.
Login Wait	The port has been disabled (for 60 seconds) because an incorrect password has been entered, or because a dial-back attempt has failed.

Logout	The port is being logged out. PORT
Password	The port is waiting for a user/application to enter the password that is required by a password-protected port.
PPP	The port is in PPP mode.
Reset	The port is reverting to its stored configuration.
Retry Connect	The port is trying to connect to a service that was previously unavailable (used when PORT AUTOCONNECT is set to ENABLED).
Running Script	The port is executing the commands contained in a script file.
Second Dialback Login	The port is making its second attempt to locate a dial-back script (the port searches the directory path "above" the path specified for this script server).
Slip	The port is a SLIP port.
Suspended	The user has entered the local-switch character, and the session is being suspended.
PPP	The port is in PPP mode.

Test Wait	The port is performing a TEST SERVICE command.
Test Out	The port is outputting the results of a TEST SERVICE command. PORT
Wait Input	The port is at the local prompt (waiting for the user to enter a command).
Wait Logout	The port is waiting for modem control signals to be deasserted.
Wait Output	The port is completing display output before logging out.
Wait Queue	A connection request from this port is in a queue.
Wait Session	The session is being disconnected.
Services Offered	The local LAT service(s) that the access server offers at the port.

SHOW/LIST/MONITOR PORT TELNET CHAR Privilege: See Below

Use these commands to view the PORT current values for Telnet ports that have been defined by the user or the access server manager.

Privilege

Secure and non-privileged users can use SHOW PORT commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORT command.

Syntax

```
SHOW/LIST/MONITOR PORT [port-list] TELNET CHARACTERISTICS
                       [ALL]
```

Where	Means
port-list	Specifies the port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.
ALL	Display the requested information about all ports.

Example

```
Xyplex>> show ports telnet char

Port 6:                                          08 Oct 1998  17:03:01

Abort Output Character:       None    Newline:                 CR/NULL
Attention Character:          None    Newline Filtering:          None
Default Port:                   23    Query Character:            None
Echo Mode:                  Remote    Remote Port:                2600
Erase Keystroke Character:    None    Synchronize Character:      None
Erase Line Character:         None    Transmit:           BuffTime  80
Interrupt Character:          None    Binary Session Mode:     PASTHRU
TerminalType:                 None    Tn3270 Device:              None
Tn3270 TranslationTable:      None    Tn3270 Printer Port:         Any
Local Port:                   4600    Tn3270 Default Port:          23


Enabled Characteristics:

Tn3270 EOR, Tn3270 TypeAhead, Telnet Pass 8D

MX1620>
```

LIST/MONITOR/SHOW PORT TELNET CHARACTERISTICS Display

The following table describes each field on the LIST/MONITOR/SHOW PORT TELNET CHARACTERISTICS display:

SHOW/LIST/MONITOR PORT TELNET CHARACTERISTICS (continued)

Field	Description
Port *n*	The number of the access server port, about which the system is displaying information. The variable *n* represents the number of a physical access server port.
user-name	The text which follows the port number shows either the name given by the user to log on to the port, or the name given to the port using the SET/DEFINE PORT USERNAME command.
Abort Output Characte	The character that, when typed in a Telnet session, causes the access server to terminate further display of output (e.g., text file), or NONE if this not defined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B). The default setting is NONE.
Attention Character	The character that, when typed in a Telnet session, causes the host to return to the operating system prompt, or NONE if this is not defined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B). The default setting is NONE.
Default Port	The default telnet port number (protocol or physical port number).
Echo Mod	Shows which connection partner in a Telnet session will echo (return to the video display or printer) characters that the user has typed at the keyboard. The possible values are: LOCAL, REMOTe, LINE, CHARACTER, PASSIVE, NOECHO, or DISABLED. The default setting is REMOTE.
Erase Keystroke Character	The character that, when typed in a Telnet session, causes the access server to delete the character immediately to the left of the cursor, or NONE if this is not defined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B). The default setting is NONE.
Erase Line Character	The character that, when typed in a Telnet session, causes the access server to delete all data in the current line of input, backwards from the cursor position, or NONE if this is not defined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B). The default setting is NONE.
Interrupt Characte	The character that, when typed in a Telnet session, causes the access server to suspend, interrupt, abort, or terminate a user process, or NONE if this is not defined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B). The default setting is NONE.
TerminalType	A "string" containing the name of the terminal type that the server sends to a Telnet host while negotiating a Telnet session. The default setting is NONE.
TN3270 TranslatonTable	The language translation table used at this port during a TN3270 session. The access server software includes one default table (USENGLSH), but you can define others. The default setting is NONE.

SHOW/LIST/MONITOR PORT TELNET CHARACTERISTICS (continued)

Local Port	Displays the local port's source IP port number.
Newline	The characters that the access server transmits to the connection partner in a Telnet session, when the user presses the <RETURN> key. The possible values are: CR/NULL, CR/LF, and CR.
Newline Filtering	The method, if any, that the access server uses to translate Telnet Newline sequences coming from the network and bound for this port. The possible values are: NONE, CR, CR/NULL, CR/LF, and STRIP NULL. The default setting is NONE.
Query Character	The character that, when typed in a Telnet session, causes the access server to provide a visible indication that the system is still up and running, or NONE if this is not defined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B). The default setting is NONE.
Remote Port	The telnet-port number for which the access server will accept a remote connection. This is similar to a logical address at which this physical port can be reached. The default setting is equal to [2000 + (physical-port-n*100)].

SHOW/LIST/MONITOR PORT TELNET CHARACTERISTICS (continued)

Synchronize Character	The character that, when typed in a Telnet session, allows the to regain control of a "runaway" process, or NONE if this is not defined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B). the default setting is NONE.
Transmit	The local port's send/transmit setting. The possible values are BUFFTIME, IMMEDIATE and IDLETIME. The default setting is BUFFTIME 80.
Binary Session Mode	The session mode that will be used when the port negotiates the Telnet binary mode. The possible values are INTERACTIVE, PASSALL, and PASTHRU. The default setting is PASTHRU.
TN3270 Device	The device type used at this port during a TN3270 session. The valid values are: TN3270_Device, TN3270 Printer_Port (ANY is the default) or TN3270 Default_Port (port 23 is the default). Use the SET PORT <*port number*> TELNET TN3270 command.

SHOW/LIST/MONITOR PORT TELNET CHARACTERISTICS (continued)

Enabled Characteristics:

Note: By default, no additional Telnet settings are enabled. If this is the case, this field is empty. Additionally, you can enable the following Telnet settings:

TN3270 EOR	An end of record is required before binary negotiation when establishing a TN3270 session.
XTDATTRS	Extended attributes are enabled at this TN3270 port.
Tn3270 ErrorLock	During a TN3270 session, the terminal will lock when you press an incorrect key sequence until you press the Reset key.
Tn3270 Space_Insert	Enables Insert mode on filled fields using the TN3270 Insert Mode.
Tn3270 TypeAhead	Specifies the size of the TN3270 typeahead buffer (the number of bytes or characters that can be temporarily stored pending transmission) for sessions at the port(s) specified in the port list.
Tn3270PREFIXKEYMAP	Allows for prepending multiple key sequences to form a Tn3270 key.
Tn3270 SCANNER	A specialized TN3270 feature that allows an OCS scanner to connect to a Tn3270 session.
Telnet Pass 8D	The will pass to the to the Telnet connection partner at 8 bits, even parity. It will not be converted.

SHOW/LIST PORT TELNET COMPORTCONTROL CHAR Privilege: See Below

Use these commands to display the current Telnet Comport settings for the specified ports.

Privilege

Secure and non-privileged users can use SHOW PORT commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORT command.

Syntax

```
SHOW/LIST PORT [port-list] TELNET COMPORT CONTROL CHARACTERISTICS
               [ALL]
```

```
MX1620> SHOW PORT 6 TELNET COMPORTCONTROL CHAR


Port 6:                                          14 Oct 1998  13:18:02

Telnet Com Port Control Client           Telnet Com Port Control Server
-------------------------------------    ----------------------------
Client:                          Disabled   Server:               Disabled

Client Toggles DTR:              Disabled
Server Raises DTR:               Disabled
```

SYNTAX

```
SHOW PORT 6 TELNET COMPORTCONTROL CHARACTERISTICS
```

Where	Description
Telnet Com Port Control Client	If enabled, the client will control the DTR signal on the port. The default setting is disabled.
Telnet Com Port Control Server	If enabled, the server will control the DTR signal on the port. The default setting is disabled.
Client Toggles DTR	If enabled, the client will request that the server raise or lower its DTR signal on the port. The default setting is disabled.
Server Raises DTR	If enabled, the server will request that the client raise or lower its DTR signal on the port. The default setting is disabled

SHOW/MONITOR QUEUE — Privilege: See Below

Use these commands to display the access server LAT service connection queue, which is a list of requests for connection to LAT services that are offered at the access server. Typically, you will use the SHOW/MONITOR QUEUE display to examine information about queued connection requests, estimate the effect of deleting entries (i.e., using a REMOVE QUEUE command), or determine the current size of the connection queue in order to adjust the SERVER QUEUE LIMIT setting.

The connection queue services requests in first-in-first-out (FIFO) order. When a connection request is queued, the access server assigns the request an entry number (i.e., job number) and a position number (i.e., first, second, third, etc). Although entries are processed in FIFO order, a connection request can be dequeued (connection is established) ahead of other entries which have a lower position number, depending on port availability.

Privilege

Secure and non-privileged users can use SHOW PORT commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORT command.

Syntax

```
SHOW/MONITOR QUEUE      [ALL]
                        [ENTRY entry-number]
                        [NODE node name]
                        [PORT port number]
                        [SERVICE service-name]
```

Where	Means
ALL	All connection request entries in the access server connection queue display. This is the default if a keyword is not types after ALL.
ENTRY	Only a specific connection request that is in the access server connection queue.
entry-number	Specify the entry number in the connection queue about which you want information.
NODE	The display will list only those connection request entries that originated at a specific node.
node name	The name of a node where the connection request entries originated.

PORT — The display will list only those connection requests that are made to a specific destination port on the access server. ,

port number — The number of the port to which the connection request was made. (Note that this could be all connection requests if only one port on the access server has queuing enabled.)

SERVICE — The display will list only those connection requests made to a LAT specific service offered by the access server.

service-name — The name of the LAT service offered by the access server.

Example

```
Xyplex>> SHOW QUEUE ALL

 Position  Entry  Source Node        Service          Port Name

   1        111   FINANCEVAX         LASER
   2        115   FINANCEVAX                          3
   3        116   ENGINEERING        MODEM            4  PORT_4
```

Example SHOW/MONITOR QUEUE Display

The following table describes each field on the SHOW/MONITOR QUEUE display:

Field	Description
Position	The current placement of each entry in the connection , . This is an indication of the relative order of each entry.
Entry	The entry number (e.g., the job number) of each queued request.
Source Nod	The name of the service node which made the connection request that is in the queue.
Service	The name of the requested service.
Port Name	The port number and/or name of the port where the requested service is offered. Information only appears in this column if a port name was specified in the connection request.

SHOW/LIST/MONITOR SERVER - General Information

Use the SHOW SERVER or MONITOR SERVER command to display information about operational database parameters for the server. Use the LIST SERVER command to display information about permanent database parameters for the server. The SHOW and LIST SERVER command produces a static display. The MONITOR SERVER command produces a display that is continuously updated.

Non-privileged users can use the SHOW and LIST SERVER command. Only users at privileged ports can use the MONITOR SERVER command.

SHOW/MONITOR SERVER ACCOUNTING Privilege: See Below

Use these commands to view the accounting log which contains information about successful and attempted connections made to or from the unit, as well as information about sessions that are disconnected. Using verbose accounting, the log will also contain information about PPP and SLIP (including compressed SLIP or CSLIP) connections, and informational messages about daemon activity and nested menu file errors. This display can be useful in identifying the cause of problems that are occurring on the server.

Privilege

Secure and non-privileged users can use SHOW PORT commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORT command.

Syntax

```
SHOW/MONITOR SERVER ACCOUNTING
```

Example

```
Xyplex>> show server accounting
ENTRY ADDRESS          PORT USERNAME         TYPE DESTINATION       CONNECT TIME          DISCONNECT TIME       BYTES IN BYTES OUT
    1 08-00-87-03-34-6B   0 (Remote)         -Rtm 140.179.133.136   07 Oct 1998 15:56:52
    1 08-00-87-03-34-6B   0 (Remote)         D 0  140.179.133.136   07 Oct 1998 15:56:52  07 Oct 1998  16:00:09  8180       166
    2 08-00-87-03-34-6B   0 (Remote)         -Rtm 140.179.133.136   08 Oct 1998 08:28:46
```

SHOW SERVER ACCOUNTING DISPLAY (Default Accounting)

```
Xyplex>> show server accounting
23 Sep 1998 13:28:20 SLIP Link Startup on Port 11
23 Sep 1998 13:28:46 FINGERD request from 140.179.192.3
23 Sep 1998 13:28:46 FINGERD request :
23 Sep 1998 13:29:13 source:08-00-87-01-CB-A4 dest:140.179.192.3 port:0 user:(Remote) type:Rtelm
23 Sep 1998 13:29:13 source:08-00-87-01-CB-A4 dest:140.179.192.3 port:0 user:(Remote) type:D reason:0 bytes in:1 bytes out:0
23 Sep 1998 13:30:51 source:08-00-87-01-CB-A4 dest:140.179.50.201 port:0 user:(Remote) type:Rtelm
```

SERVER ACCOUNTING DISPLAY (Verbose Accounting)

The following table describes each field related to connections in the MONITOR/ SHOW SERVER ACCOUNTING display:

Field	Description
Entry (default display only)	The log entry number.
Address (default display) or source (verbose display)	The Ethernet address of the server.

Port	The port from or to which the connection is made.
Username (default display) or user (verbose display)	The name of the user who is logged on to the port.
Type	Indicates if the connection is a local access connection or a remote access connection, or if a connection has been disconnected, a reason for the disconnect. Valid Connections types are: L Local access. R Remote access. D Disconnect. The letter "D" is followed by a number which represents the reason why the disconnect occurred (see Disconnect Codes on next page). The following list describes the possible connection types:

Default	Verbose	Connection Type
la	lat	LAT
te	telnet	Telnet
lt	lat/tel	LAT/Telnet
tn	tn3270	TN3270
rn	rcpn	Remote console via node name
rp	rcpp	Remote console via physical port
rl	rlogin	RLOGIN
lq	latq	Queued LAT connection
tm	telm	Telnet maintenance
xr	xrem	XREMOTE
xp	xprn	XPRINTER (IPX)

Destination	The connection's destination LAT service name, domain-name, or internet-address.
Connect Time	The time the connection was made. For Verbose, this field's "title" is not displayed, just displays the date/time stamp.
Disconnect Time	The time the connection was disconnected. For Verbose, this field's "title" is not displayed, just displays the date/time stamp.
Bytes In	The number of bytes of data that the port received from the device.
Bytes Out	The number of bytes of data output by the port to the device.

reason — Disconnections are indicated by the letter D, followed by a reason number which represents the reason why the disconnection occurred The following table lists the error codes and the corresponding reason for a session being disconnected.

Disconnect Codes

Code	Related Error Code	Connection terminated or refused because…
0	None - normal disconnection	The user logged out or disconnected the port.
1	**211 or 251**	The server received messages that violate the LAT protocol.
2	**212 or 252**	The server received messages that violate the LAT protocol.
3	**213 or 253**	The server received messages that violate the LAT protocol.
4	**214 or 254**	The server received messages that violate the LAT protocol.
5	**215 or 255**	The queue entry id already exists in the queue.
6	**216 or 256**	The LAT virtual circuit is now inactive.
7	**217 or 257**	The server had insufficient memory or resources to make the connection.
8	**218 or 258**	The service node (a host or a remote access server offering the service) would not permit the connection.
9	**219 or 259**	The service is no longer available.
10	**220 or 260**	Your server would not permit the connection.
11	**221 or 261**	The server had insufficient memory or resources to make the connection.
12	**222 or 262**	The server is being reinitialized or shut down.
13	**223 or 263**	The remote node offering the service intentionally aborted the connection.
14	**224 or 264**	The LAT circuit timer at your server is not set appropriately.
15	**225 or 265**	The server received messages that violate the LAT protocol.
16	**226 or 266**	The server received messages that violate the LAT protocol.

Code	Related Error Code	Connection terminated or refused because…
17	**227 or 267**	The service node failed to respond within the time period defined by DEFINE/SET SERVER RETRANSMIT LIMIT setting.
18	**228 or 268**	The server determined that no progress was being made on the existing virtual circuit. This is an indication of how busy the service node is.
19	**229 or 269**	The service is not offered on the requested port.
20	**230 or 270**	The service is not offered on the requested port.
21	**231 or 271**	You specified an incorrect password.
22	**232 or 272**	The requested service is already being used.
23	**233 or 273**	The requested service is no longer offered at your server.
24	**234 or 274**	The service is disabled.
25	**235 or 275**	Connection was not in the connection queue.
26	**236 or 276**	That server is not configured for queued access.
27	**237 or 277**	Access violation.
28	**238 or 278**	The server received messages that violate the LAT protocol.
29	**none**	An unexpected event.
30	**735**	The service specified in a TEST SERVICE command does not support the specified test.
31	**793**	The domain-name is too long or in an invalid format.
32	**710**	The requested service is not offered at the node specified, or the service or node name that you specified is not known to the server.
33	**711**	The service specified is unknown to the unit, the server node limit has been reached, the server is unable to store information about additional nodes, or you are not authorized to use the service specified.
34	**none**	Connection was rejected.
35	766	Attempted to connect to an internet-address from a port that has DEFINE/SET PORT IP CONNECTIONS disabled.
36	240	The TCP port number is unavailable.

SHOW/MONITOR SERVER ALTERNATE STATUS Privilege: See Below

Use these commands to view the current values for server processor and memory usage.

Privilege

Secure and non-privileged users can use SHOW SERVER commands. Only users at privileged ports can use the MONITOR SERVER command.

Syntax

SHOW/MONITOR SERVER ALTERNATE STATUS

Example

```
Xyplex>> show server alternate status

MX1620 V6.0.4S10 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 1 18:58:11
Address:   08-00-87-03-34-6B   Name:   X03346B             Number:     0
Protocol(s):   LAT, TELNET, RLOGIN, SNMP, PPP, IPX, XPRINTER
Daemon(s):     LPD

Installed Memory:  4194304 bytes
Crate Current State:        N/A             Crate Transition Count:    N/A
Time Received From:  140.179.147.70

                        Cur    High     Max  Failures  Last Occurred
Processes:               57      57     200         0
Timers:                  56      58     255         0
Packet Buffers:          16      47      80         0
IPC Messages:             0       0      32         0

                        Cur     Low     Max  Failures  Last Occurred
Free Text Pool:       12240   12176   16384         0
Free Memory:        1993168 1978256 2011104         0

Total Fragment(s) = 9  Start    Size       Start    Size       Start    Size
                    1) 9A19E0 1986912   2) 9043E0    5904   3) 904050     256
                    4) 9070F0     112   5) 9068F0     112   6) 9065C0      32
                    7) 8B5140      32   8) 88C560      32   9) 844650      32
```

MONITOR/SHOW SERVER ALTERNATE STATUS Display

The following table describes each field on the MONITOR/SHOW SERVER ALTERNATE STATUS display

SHOW/MONITOR SERVER ALTERNATE STATUS (continued)

Where	Means
Cur	The level or amount of the resource that is currently in use.
High	The highest amount of the resource used since the server was last initialized.
Max	The maximum amount of the resource that can be used (either because of a hardware constraint or because the value shown is the value specified for a server setting).
Failures	The number of times a failure has occurred for a given resource.
Last Occurred	The most recent occurrence of a failure for a given resource.
Protocol(s)	The protocols available on your server. Valid values are: LAT, TELNET, TN3270, RLOGIN, SNMP, PPP, IPX, XREMOTE and XPRINTER.
Daemon	The current Daemon setting. Valid values are: FINGERD, LPD, ROUTED, RWHOD and SYSLOGD.
Installed Memory	Display the unit's installed memory.
Crate Current State	For Network 9000 units, shows whether or not any modules are currently experiencing a fault. For chassis that have the Redundant Power Supply, this field can also indicate a fault with one of the power supplies. A "No Fault" message means that there are currently no faults.
Crate Transition Count	The number of times a fault has occurred or has been cleared. This indicates how well the server is operating under the current load, and may be helpful in identifying network trouble or server problems. For each server resource listed, the display shows:
Time Received From	Shows the IP address of the Host that provides the time of day to the server.
Processes	The number of processes (for example, user sessions, server "housekeeping" activities, user command line interfaces, etc.) occurring on a server.
Timer	The number of timers (internal to processes) that are currently in use by the processes that are currently active on the server.
Packet Buffers	The number of incoming and outgoing packets that are being buffered in server memory.

IPC Messages	The number of interprocess communication (IPC) messagesbeing ports passed among processes that are active on the server. For example, an IPC message is passed when a user session is terminated. The LAT or TCP/IP process running on the server passes a message indicating that the process has ended to the user interface process, which then informs the user of this event.
Free Text Pool	The amount of space used by the server to store identification strings for nodes, LAT services, and domain names (which is referred to as text pool space), as well as the number of times an operation was attempted, but for which there was insufficient text pool space, and when the last failure occurred. If there are Text Pool Failures, you should consider increasing the size of the SERVER TEXTPOOL SIZE setting, or adjusting the number or size of the identification strings for nodes, LAT services, and domain names that the server must store.
Free Memory	The amount of memory available, the number of times an operation was attempted, but for which there was insufficient non-text pool space, and when the last failure occurred. If there are Free Memory Failures, you should consider decreasing the size of the SERVER TEXTPOOL SIZE setting, or adjusting the number of the nodes, LAT services, and domain names that the server must store.
Total Fragment(s)	The number of unused fragments of server memory and the largest of these fragments. The number shown in the "Start" column is the hexadecimal memory address of the fragment. The number shown in the "Size" column is the size of the fragment, in bytes

SHOW/LIST SERVER ARAP CHARACTERISTICS Privilege: N, P

Use these commands to view information about the settings that are currently specified for various ARAP characteristics, and at which ports the ARAP feature is enabled.

Syntax

```
SHOW/LIST SERVER ARAP CHARACTERISTICS
```

Example

```
Xyplex> show server arap characteristics

ARAP Node:           REMOTEMAC
ARAP Default Zone:   REMOTEZONE
ARAP Current Zone:   AppleTalk
ARAP Port settings:          1, 2, 3
```

SHOW SERVER ARAP CHARACTERISTICS Display

The following table describes the fields on the SHOW/LIST SERVER ARAP CHARACTERISTICS display:

Field	Description
ARAP Node	The server's AppleTalk name.
ARAP Default Zone	The name of the AppleTalk/EtherTalk zone that the server will attempt to join when it is initialized.
ARAP Current Zone:	The name of the AppleTalk zone to which the server currently belongs. (This field displays only when you use the SHOW command.)
ARAP Port settings:	The ports where the ARAP feature is enabled.

SHOW SERVER CCL — Privilege: N, P

Use this command to display the names of loaded CCL scripts and the ports to which they are assigned.

Syntax

```
SHOW [SERVER] CCL ["ccl-name"]
                  [ALL]
```

Where	Means
ccl-name	The ports where a specific CCL script is loaded.
ALL	Lists all CCL scripts that are loaded at port on this server, and indicates which ports the scripts are loaded on. This is the default.

Example

```
Xyplex> show server ccl all

CCL script "SupraFAXModem_V.32bis" loaded, not used by any port
CCL script "ZOOMV32.ARA" loaded, not used by any port
CCL script "Telebit_T3000" loaded, in use by port(s) 1 2
```

SHOW SERVER CCL Display

SHOW/LIST/MONITOR SERVER CHARACTERISTICS Privilege: See Below

Use the SHOW/LIST/MONITOR SERVER CHARACTERISTICS command to view the current or permanent server settings defined by the server manager. This is the default display type.

Privilege

Secure and non-privileged users can use SHOW and LIST SERVER commands. Only users at privileged ports can use the MONITOR SERVER command.

Syntax

```
SHOW/LIST/MONITOR SERVER CHARACTERISTICS
```

Example

```
Xyplex>> show server characteristics

MX1620 V6.0.4S10 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 1 18:59:42
Address:   08-00-87-03-34-6B   Name:   X03346B              Number:     0

Identification:  Xyplex Access Server
Welcome:         Welcome to the Xyplex Access Server.

Circuit Timer:            80           Password Limit:            3
Console Port:              0           Queue Limit:              24
Inactivity Timer:         30           Retransmit Limit:          8
Keepalive Timer:          20           Session Limit:            64
Multicast Timer:          30           Software:           XPCSRV20
Node Limit:              100           Identification Size:      63
Textpool Size:         16384           Timezone:              00:00
Accounting Entries:      250           Packet Count:             80
Nested Menu Size:          0           Menu Name:
Userdata Delay:           50           IPX Internal Net:   58504C58
IPX Protocol:  Ethernet                Xprinter Timeout:         15
Service Groups: 0
Time Server: 0.0.0.0          Disabled
Enabled Characteristics:
Announcements, Broadcast, Change, Console Logout, Dump, Lock,
Parameter Polling, TFTP Parameters, Proprietary Parameters,
TFTP Read Broadcasts, Purge Node
```

LIST/MONITOR/SHOW SERVER CHARACTERISTICS Display

The following table describes the fields on the LIST/MONITOR/SHOW SERVER CHARACTERISTICS display:

SHOW/LIST/MONITOR SERVER CHARACTERISTICS (continued)

Field	Description
Identification	Text message that identifies the server.
Welcome	The text message that is displayed when a user logs on to the server.
Circuit Timer	The amount of time (in milliseconds) between the transmission of messages to service nodes.
Console Port	The number of the port that acts as the console port for server messages.
Inactivity Timer	The amount of time (in minutes) that a port can remain logged in to the server and have no connected sessions, before the port is logged off.
Keepalive Timer	The amount of time (in seconds) the server will wait before it transmits a null message on an active virtual circuit to service nodes (for the purpose of notifying these nodes that the server is still available on the network).
Multicast Timer	The amount of time (in seconds) between transmission of multicast announcements to indicate the availability of local services.
Node Limit	The maximum number of service nodes about which the server can retain information.
Textpool Size	The maximum amount of server memory that is reserved for storing identification strings for nodes, LAT services, and domain names.
Accounting Entries	The maximum number of entries that can be contained in the server accounting log.
Nested Menu Size	The amount of memory (in bytes) currently reserved for nested menus. The default of 0 disables the feature.
Userdata Delay	How long the port should delay before sending the user data to the connection partner after the connection is established. Valid *delay-values* are 0 to 3000. Each number represents 10 milliseconds. So, for example, the number 255 translates into a delay of 2550 ms, or 2.55 seconds. The default is 50 (500 ms).
IPX Protocol	The type of packets (Ethernet or MAC (IEEE 802.3)) used for IPX printing.

SHOW/LIST/MONITOR SERVER CHARACTERISTICS (continued)

Service Groups	The authorized groups that have access to services at this server.
Time Server	The IP address of the server that is supplying the time to the unit. Also indicates whether this feature is currently enabled or disabled. The default is 0.0.0.0 and disabled.
Password Limit	The maximum number of times that the server will allow a user to incorrectly enter a password.
Queue Limit	The maximum number of entries allowed in the server connection queue.
Retransmit Limit	The maximum number of times the server will attempt to retransmit a message that has not been acknowledged by a service node.
Session Limit	The maximum number of sessions permitted among all ports.
Software	The name of the software image at the load host.
Identification Size	The maximum length of LAT node and service identification strings that the server stores in memory.
Timezone	The time zone differential, in hours and minutes, from Universal Time (formally called Greenwich Mean Time that was passed by the load server, after loading via TFTP.
Packet Count	The current setting (in bytes) for incoming and outgoing packets. The default is 80 bytes.
Menu Name	The name of the menu file on the script server.
IPX Internal Net	The current IPX network number. The valid values are hexadecimal numbers between 1 (default) and FFFFFFFE.
Xprinter Timeout	How many seconds the print job can idle. Valid values are 15 (default) to 300 seconds.
Enabled Characteristics	The port's enabled characteristics that were set using the DEFINE/SET SERVER command. Possible values are:
	Announcements — The server will multicast an announcement to indicate that local services are available.

Broadcast	The server allows port users to use the BROADCAST command to send messages to other ports.
Change	Changes can be made to take effect both immediately and on a permanent basis when the Change is Enabled.
Console Logout	The server will immediately disconnect a console port session when the user logs out from the console port.
Dump	The unit performs a crash dump (e.g., dumps a copy of the contents of its memory into a file at the load host, and then re-initializes) when it detects that a fatal software error has occurred.
Lock	The server allows users to execute a LOCK command to secure their port while they are away.
Parameter Polling	The server can locate additional eligible parameter servers (the SERVER PARAMETER CHECK characteristic is set to ENABLED).
Proprietary Parameters	If Enabled, the server will use a Xyplex proprietary protocol to locate additional eligible parameter server.
Purge Node	If enabled, the server will remove LAT reachable nodes from the node database whenever the limit specified by the SERVER NODE LIMIT is reached.
TFTP Parameters	If enabled, the server uses TFTP to locate additional eligible parameter servers.
TFTP Read Broadcasts	If enabled, the server should send a TFTP read broadcast as well as a BOOTP broadcast to find parameter servers on the network. This is done on server initialization, when the parameter check time or a CHECK PARAMETER SERVER command is issued. The default is ENABLED.

SHOW/MONITOR SERVER COUNTERS Privilege: See Below

Use the SHOW/MONITOR SERVER COUNTERS display to view statistics about server activity, and occurrences of error conditions.

Privilege

Secure and non-privileged users can use SHOW SERVER commands. Only users at privileged ports can use the MONITOR SERVER command.

Syntax

```
SHOW/MONITOR SERVER COUNTERS
```

Example

```
Xyplex>> show server counters

MX1620 V6.0.4S10 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 1 19:00:26
Seconds Since Zeroed:       154826     Frames Sent, 1 Collision:          28
Bytes Received:          101119519     Frames Sent, 2+ Collisions:        25
Bytes Sent:                 925752     Send Failures:                      0
Frames Received:           1266759     Send Failure Reasons:      0000000000
Frames Sent:                 17921     Receive Failures:               18530
Multicast Bytes Rcv'd:   100492510     Receive Failure Reasons:   0000000000
Multicast Bytes Sent:        82378     Unrecognized Destination:       67480
Multicast Frames Rcv'd:    1259213     Data Overrun:                       0
Multicast Frames Sent:        1635     User Buffer Unavailable:            0
Frames Sent, Deferred:         153     System Buffer Unavailable:          0

Messages Received:                0     Duplicates Received:                0
Messages Transmitted:             0     Messages Re-Transmitted:            0
Solicitations Accepted:           0     Illegal Messages Rcv'd:             0
Solicitations Rejected:           0     Illegal Slots Rcv'd:                0
Multiple Node Addresses:          0     Illegal Multicasts Rcv'd:           0
Bad Packets:         0  Type:    -     Last Occurred:
```

Example MONITOR/SHOW SERVER COUNTERS Display

The following table describes each of field on the MONITOR/SHOW SERVER COUNTERS display. The values listed indicate cumulative values counted since the last time the display counters were reset to zero. There are two ways to reset these counters: use a ZERO COUNTERS command, or re-initialize the server.

SHOW/MONITOR SERVER COUNTERS (continued)

Field	Description
Seconds Since Zeroed	The number of seconds since the counters were reset to zero.
Bytes Received	The total number of bytes contained in datagrams that have been successfully received from the network by the server, excluding Ethernet header and CRC data.
Bytes Sent	The total number of bytes contained in datagrams that have been successfully transmitted to the network by the server, excluding Ethernet header and CRC data.
Frames Received	The total number of datagram frames, including multicast frames, that have been successfully received by the server.
Frames Sent	The total number of datagram frames, including multicast frames, that have been successfully transmitted by the server.
Multicast Bytes Rcv'd	The total number of bytes contained in multicast frames that have been successfully received by the server, excluding Ethernet header and CRC data.
Multicast Bytes Sent	The total number of bytes contained in multicast frames that have been successfully transmitted by the server, excluding Ethernet header and CRC data.
Multicast Frames Rcv'd	The total number of multicast frames that have been received by the server, since the counters were reset to zero.
Multicast Frames Sent	The total number of multicast frames that have been transmitted by the server.
Frames Sent Deferred	The number of times when the server deferred transmission of a frame because the data link was in use.
Frames Sent, 1 Collision	The number of times the server successfully transmitted a frame on the second attempt after a collision occurred during the first attempt.
Frames Sent, 2+ Collisions	The number of times the server successfully transmitted a frame after a collision occurred during the first two or more attempts.
Send Failures	The number of times the Ethernet interface aborted a transmission request (see Send Failure Reasons).

Send Failure Reasons

The types of problems encountered which caused send failure(s) to occur. This information is presented in the form of a cumulative mask, in which the following bits are defined (Bit 0 is the rightmost bit):

Example

```
Send Failure Reason: 0010110550
```

Bit	Definition
0	Transmission failed to complete after 16 retries.
1	Carrier lost on the Ethernet network during transmission.
4	Transmission aborted because the frame exceeded the maximum allowable length.
5	Late collision during a transmission attempt.
9	Data underflow condition.

Receive Failures

The number of packets that were received with an error (see Receive Failure Reasons).

Receive Failure Reasons

Indicates the types of problems encountered which caused receive failure(s) to occur. This information is presented in the form of a cumulative mask, in which the following bits are defined (Bit 0 is the rightmost bit):

Example

```
Receive Failure Reason: 0010110220
```

Bit	Definition
0	Block check error occurred. Indicates that the received packet did not pass the CRC check.
1	Framing error occurred. Indicates that the received packet did not contain an integral number of 8-bit bytes.
2	Message length error occurred. Indicates that the received packet exceeded 1518 bytes.

Unrecognized Destination

The number of times a frame passed through the server hardware, but the server did not recognize the address and discarded the message.

Data Overrun

The number of times the server hardware lost an incoming frame because it was unable to keep up with the data rate.

SHOW/MONITOR SERVER COUNTERS (continued)

User Buffer Unavailable	The number of times the server did not have a user buffer available.
System Buffer Unavailable	The number of times that a system buffer was unavailable to the server for an incoming frame.
Messages Received	The number of LAT virtual circuit messages that have been successfully received by the server.
Messages Transmitted	The number of LAT virtual circuit messages that have been successfully transmitted by the server.
Solicitations Accepted	The number of queued LAT connection requests that the server has accepted. This number includes both queued requests and requests that were immediately satisfied without queuing.
Solicitations Rejected	The number of queued LAT connection requests that the server could not process and has rejected.
Multiple Node Addresses	The number of times a service node became available with a different Ethernet address.
Bad Packets	The number of bad packets received.
Type	The type of bad packets received. Valid values are: IEEE 802.3 (MAC) type packets when communicating with a Novell printer server or Ethernet packets.
Duplicates Received	The number of duplicate LAT messages that the server received.
Messages Re-Transmitted	The number of LAT messages that the server retransmitted because they were not acknowledged by the destination service node.
Illegal Messages Rcv'd	The number of LAT messages that have been received by the server which have an illegal format.
Illegal Slots Rcv'd	The number of LAT messages that have been received by the server which have an illegal slot format.
Illegal Multicasts Received	The number of multicast messages that have been received by the server which have an illegal forma.
Last Occurred	The time the last packet was received.

SHOW/LIST/MONITOR SERVER IP CHARACTERISTICS Privilege: See Below

Use the SHOW/LIST/MONITOR SERVER IP CHARACTERISTICS command to view the current or permanent values related to IP addresses or address resolution for the server.

Privileges

Non-privileged users can use the SHOW and LIST SERVER IP CHARACTERISTICS commands. Only users at privileged ports can use the MONITOR SERVER IP CHARACTERISTICS command.

Syntax

```
SHOW/LIST/MONITOR SERVER IP CHARACTERISTICS
```

Example

```
MX1620> SHOW SERVER IP CHAR
1620 V6.0.4S11 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 31 17:58:18
Address:   08-00-87-03-34-6B   Name:   X03346B              Number:     0

Identification:  Don's Server

Internet Address:           140.179.245.192     Internet TTL:               64
Internet Broadcast Address: 255.255.255.255     Translation Table TTL:      60
Local Base:                 4000                Local Increment:           100
Routing Table Size:         64                  TCP Retransmit:            640
Domain Name:
Default Domain Suffix:

IP Address Auto Discovery:  DISABLED
Domain TTL:                 0                   IP Reassembly:         DISABLED
Primary Domain Address:     140.179.130.200     TCP Resequencing:      DISABLED
Secondary Domain Address:   140.179.50.201      TCP Connect Timer:           32

Primary Gateway Address:    140.179.128.1
Secondary Gateway Address:  0.0.0.0
Gateway Timeout:            60
Subnet Mask:                255.255.128.0
Subnet Mask Auto-Configure: DISABLED

MX1620>
```

Example LIST/MONITOR/SHOW SERVER IP Display

The following table describes each field on the LIST/MONITOR/SHOW SERVER IP display.

SHOW/LIST/MONITOR SERVER IP CHARACTERISTICS (continued)

Field	Description
Internet Address	The Internet address for this server. IP
Internet Broadcast Address	The Internet address that is used in Internet Broadcast messages.
Local Base	Define the local TCP port starting base for the server as well as an optional increment value. The base value is used as the local TCP port for PORT 0. Valid values are from 1 to 32767. The default value is 4000.
Routing Table Size	The current number of learned and static Internet routes that the operational Internet routing table contains. The table size can be from 64 to 512 entries. The default is 64 entries.
Domain Name	The *domain-name* by which the server is known on the network.
Default Domain Suffix	The default *domain-name-suffixes* that the server uses to develop a fully-qualified *domain-name*, whenever a user specifies an incomplete *domain-name* (the server appends the suffixes to the incomplete *domain-name*).
Internet TTL	The maximum amount of time, in seconds, that an Internet data packet can circulate through the network before the packet is discarded (i.e., "time to live".
Translation Table TTL	The time-to-live (in seconds) for unreferenced translation table entries. The valid values are 0 - 255 seconds. The default is 60 seconds.
Local Increment	The optional increment value for the TCP port starting base for the server. The valid increment values are from 1 to 1024. The default value is 100.
TCP Retransmit	The initial TCP retransmit timeout value. This is the time at which TCP initially retransmits unacknowledged segments. A value between 600 and 3000 milliseconds. 640 is the default setting.
IP Address Auto Discovery	If enabled, the server will be able to obtain its working IP address in a non-standard method. Contact Xyplex Support for more information on this parameter.

SHOW/LIST/MONITOR SERVER IP CHARACTERISTICS (continued)

Domain TTL	The number of hours that a *domain-name* will be retained by the server.
Primary Domain Addres/ Secondary Domain Address	The *internet-address* at which a Domain name server is located. Domain name servers are network objects where the network attempts to resolve a domain-name. The server can use up to two Domain name servers (primary and secondary) to resolve a domain-name. The server will query both the primary and secondary Domain servers (at the same time) to resolve a domain-name.
IP Reassembly	If enabled, the server reassembles packets that it receives that were fragmented by a gateway or router.
TCP Resequencing	If enabled, shows that the server will accept packets received out of sequence.
TCP Connect Timer	Specify how many seconds TCP will try to form a connection. The valid values are 4 to 32 seconds. The default value is 32 seconds.
Primary Gateway Address Secondary Gateway Address	The internet-address at which an Internet gateway is located. The server can use up to two Internet gateways (primary and secondary) to locate a device on an external network. The server will use the address of the primary gateway to route a transmission to a remote device, until it determines that the primary gateway has failed. Then the server will use the address of the secondary gateway
Gateway Timeout	How often (in seconds) the primary gateway is being ping'd to determine its status.
Subnet Mask	The Internet subnet-maskwhich server uses to distinguish Internet addresses that can be reached directly from those that must be reached via an IP Gateway.
Subnet Mask Auto-Configure	Shows whether or not the software will use an *internet-subnet-mask* specified by the server manager, or one that has been determined automatically by the server. Enabled means that the server will automatically determine the *internet-subnet-mask*. Disabled means that the server will use an *internet-subnet-mask* specified by the server manager.

SHOW/MONITOR SERVER IP COUNTERS Privilege: See Below

Use the SHOW/MONITOR SERVER IP COUNTERS display to view statistics about server IP, TCP, and UDP activity, and occurrences of error conditions .

Privileges

Non-privileged users can use the SHOW and LIST SERVER IP COUNTERS commands. Only users at privileged ports can use the MONITOR SERVER IP COUNTERS command.

Syntax

```
SHOW/MONITOR SERVER IP COUNTERS
```

Example

```
Xyplex>> show server IP counters
MX1620 V6.0.4S10 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 1 19:02:09

Internet Address:  140.179.245.192
Domain Name:
Domain Suffix:



IP Packets Received:          130168       IP Packets Transmitted:        8414
IP Checksum Errors:                0       IP Header Errors:                 0
IP Fragments Received:             0       IP Rx Delivery:               61958
IP Unknown Protocol Rcvd:      64409       IP Deliveries Rcvd:           65515
IP Failed Reassemblies:            0       IP No Routes Sent:                0
Frags Not Accepted:                0       Frags on Reassembly Que-High:     0

TCP Packets Received:           3766       TCP Packets Transmitted:       7238
TCP Retransmissions:               0       TCP Checksum Errors:              0
TCP Active Opens:                  0       TCP Passive Opens:                2
TCP Failed Attempts:               0       TCP Establish Resets:             0
TCP Total Resets:                  7       Current TCP Segments Queued:      0
TCP Packets Discarded:             0

UDP Messages Received:          2941       UDP Messages Sent:              676
UDP No Port Messages Rcvd:     58280       UDP Receive Message Errors:       0
```

Example MONITOR/SHOW SERVER IP COUNTERS Display

The following table describes each of the fields on the MONITOR/SHOW SERVER IP COUNTERS display:

Field	Description
Internet Address	The Internet address for this server.
Domain Name	The domain-name by which the server is known on the network.
Domain Suffix	The default *domain-name-suffixes* that the server uses to develop a fully-qualified *domain-name*, whenever a user specifies an incomplete *domain-name* (the server appends each of the suffixes in turn to the incomplete *domain-name*, until a successful resolution is made).
IP Counters	
IP Packets Received	The total number of IP packets (i.e., the sum of all TCP packets, UDP packets, and ICMP packets) received by the server, since the counters were reset to zero.
IP Checksum Errors	The number of times the server received an IP packet containing a checksum error, since the counters were reset to zero.
IP Fragments Received	The number of times that the server received an IP fragment, since the counters were reset to zero.
IP Unknown Protocol Rcvd	The number of times that the server received an IP packet that was not a TCP, UDP, or ICMP packet.
IP Failed Reassemblies	The number of times that the server discarded an IP message because the server did not receive all of the fragments which were part of the message, within a specified period of time.
Frags Not Accepted	The number of times that the server discarded a packet that it received that was fragmented by a gateway or router.
IP Packets Transmitted	The total number of IP packets (i.e., the sum of all TCP packets, UDP packets, and ICMP packets) transmitted by the server, since the counters were reset to zero.
IP Header Errors	The number of times the server received an improperly formatted IP packet, since the counters were reset to zero.
IP Rx Delivery	The number of times that the server could not deliver an IP packet to a higher level protocol.

IP Deliveries Rcvd	The number of times that the server could deliver an IP packet to a higher level protocol.
IP No Routes Sent	The number of times that the server could not send an IP packet because the server did not know how to reach the destination.
Frags on Reassembly Que-High	The number of highest number of packets that were received out of sequence that the server stored.

TCP Counters

TCP Packets Received	The total number of TCP packets received by the server, since the counters were reset to zero.
TCP Retransmissions	The number of times the server had to retransmit a TCP packet, since the counters were reset to zero.
TCP Active Opens	The number of TCP virtual circuits that were initiated by the server
TCP Failed Attempts	The number of times that the server was unable to open a TCP virtual circuit.
TCP Total Resets	The number of TCP virtual circuits the server aborted or refused.
TCP Packets Discarded	The total number of TCP packets discarded by the server, since the counters were reset to zero.
TCP Packets Transmitted	The total number of TCP packets transmitted by the server, since the counters were reset to zero.
TCP Checksum Errors	The number of times the server received a TCP packet containing a checksum error, since the counters were reset to zero.
TCP Passive Opens	The number of TCP virtual circuits that were initiated by the remote connection partner.
TCP Establish Resets	The number of times that the remote connection partner aborted an established TCP virtual circuit with the server.
Current TCP Segments Queued	If TCP resequencing is enabled, the number of segments currently queued for resequencing.

UDP Counters

UDP Messages Received	The total number of UDP packets received by the server, since the counters were reset to zero.
UDP No Port Messages Rcvd	The number of times that the server received a UDP message that was addressed to an invalid UDP port on the server.
UDP Messages Sent	The total number of UDP packets transmitted by the server, since the counters were reset to zero.
UDP Receive Message Errors	The number of times that the server received a UDP broadcast message, and discarded the message.

SHOW/LIST/MONITOR SERVER IP ICMP COUNTER Privilege: See Below

Use the SHOW/MONITOR IP SERVER ICMP COUNTER display to view statistics about server ICMP activity, and occurrences of ICMP error conditions. **Error! Bookmark not defined.**

Privileges

Non-privileged users can use the SHOW and LIST SERVER IP ICMP COUNTER commands. Only users at privileged ports can use the MONITOR SERVER IP TCMP COUNTER command.

Syntax

```
SHOW/MONITOR SERVER INTERNET ICMP COUNTER
```

Example

```
Xyplex>> show server ip icmp counter
MX1620 V6.0.4S10 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 1 19:02:57

Internet Address:  140.179.245.192
Domain Name:
Domain Suffix:


ICMP Messages Received:          531       ICMP Messages Sent:             509
Destination Unreachable Rcvd:     22       Destination Unreachable Sent:     0
Time-to-live Exceeded Rcvd:        0       Time-to-live Exceeded Sent:       0
Parameter Problem Rcvd:            0       Parameter Problem Sent:           0
Source Quench Rcvd:                0       Source Quench Sent:               0
Redirect Rcvd:                     0       Redirect Sent:                    0
Echo Rcvd:                       509       Echo Reply Sent:                509
Timestamp Rcvd:                    0       Timestamp Reply Sent:             0
Information Request Rcvd:          0       Information Reply Sent:           0
Unknown Messages Rcvd:             0
```

MONITOR/SHOW SERVER IP ICMP COUNTER Display

Note: *The totals in these fields only reflect the server activity information since the last time the counters were reset to zero.*

The following table describes each field on the MONITOR/SHOW SERVER IP ICMP COUNTER display

Field	Description
Internet Address	The Internet address for this server.
Domain Name	The *domain-name* by which the server is known on the network.
Domain Suffix	The default *domain-name-suffixes* that the server uses to develop a fully-qualified *domain-name*, whenever a user specifies an incomplete *domain-name* (the server appends the suffixes to the incomplete *domain-name*).
ICMP Messages Received	The total number of ICMP packets received by the server.
Destination Unreachable Rcvd	The number of times that the server received an ICMP message indicating that a destination was unreachable.
Time-to-live Exceeded Rcvd	The number of times that the server received an ICMP message indicating that an IP packet has exceeded its time to live.
Parameter Problem Rcvd	The number of times that the server received an ICMP message from a node indicating the server sent an improperly formatted IP packet.
Source Quench Rcvd	The number of times that the server received an ICMP message from a node, indicating that the node is temporarily unable to accept further data.
Redirect Rcvd	The number of times that the server received an ICMP message from a gateway, indicating that there is a better path by which the server can route a packet.
Echo Rcvd	The number of times that the server received an ICMP Echo message.
Timestamp Rcvd	The number of times that the server received an ICMP message requesting the current time.
Information Request Rcvd	The number of times that the server received an ICMP message requesting the number of the network to which the server is connected.
Unknown Messages Rcvd	The number of times that the server received an undefined ICMP packet.

SHOW/LIST/MONITOR SERVER IP ICMP COUNTER (continued)

ICMP Messages Sent	The total number of ICMP packets transmitted by the server .
Destination Unreachable Sent	The number of times that the server transmitted an ICMP message indicating that a destination was unreachable.
Time-to-live Exceeded Sent	The number of times that the server transmitted an ICMP message indicating that an IP message has exceeded its time to live.
Parameter Problem Sent	The number of times that the server has transmitted an ICMP message indicating that it has received an improperly formatted IP packet.
Source Quench Sent	The number of times that the server transmitted an ICMP message to a node, indicating that it is temporarily unable to accept further data.
Redirect Sent	The number of times that the server transmitted an ICMP message indicating that there is a better path by which a packet can be routed.
Echo Reply Sent	The number of times that the server responded to an ICMP Echo message.
Timestamp Reply Sent	The number of times that the server responded to a request for the current time.
Information Reply Sent	The number of times that the server transmitted an ICMP message in response to a request for the number of the network to which the server is connected

SHOW/LIST/MONITOR SERVER IP ROTARY Privilege: See below

Use the SHOW/LIST/MONITOR SERVER IP ROTARY display to view a list of rotaries contained in the operational or permanent database.

Privileges

Non-privileged users can use the SHOW and LIST SERVER IP ROTARY commands. Only users at privileged ports can use the MONITOR SERVER IP ROTARY command.

Syntax

```
SHOW/LIST/MONITOR SERVER IP ROTARY
```

Example

```
Xyplex>> show server internet rotary
        Round Robin search: DISABLED, Search by first available
        Internet Address         Ports

         140.179.245.192         0-20
```

SHOW/MONITOR/LIST SERVER IP ROTARY Display

The first column of the SHOW/MONITOR/LIST SERVER IP ROTARY display lists the internet-address assigned to the port(s) that are listed in the second column.

SHOW/LIST/MONITOR SERVER IP ROUTES Privilege: S, N, P

Use the SHOW/LIST/MONITOR SERVER IP ROUTES command to display a list of one or all internet-routes contained in the operational or permanent database.

Privileges

Non-privileged users can use the SHOW and LIST SERVER IP ROUTES commands. Only users at privileged ports can use the MONITOR SERVER IP ROUTES command.

Syntax

```
SHOW/LIST/MONITOR SERVER IP ROUTES        [ALL]
                                          [destination]
                                          [entry]
```

Where	Means
ALL	The server will display a list of all internet-routes contained in the operational or permanent database.
destination	The server will display the internet-route entry information for a specific destination.
entry	The server will display only the specific operational or permanent database internet-route entry. Valid values are 1 through 64.

Example

```
Xyplex>> show server internet routes
        Address         Gateway          Mask                 Last Modified
1 192.12.119.255      128.6.201.7    255.255.255.0         NET/FIXED 21 Mar 1998 09:22
2 192.12.120.21       128.6.201.8          0.0.0.0         HOST/VAR  24 Mar 1998 13:58*
```

SHOW/MONITOR/LIST SERVER IP ROUTES Display

The first column of the SHOW/MONITOR/LIST SERVER IP ROUTES display lists the entry number for each internet route. The following table describes the remaining columns:

Field	Description
Address	The *internet-address* of the destination host or network.
Gateway	The *internet-address* of the gateway to which traffic is sent.
Mask	The mask that the server uses to determine the network portion of the *internet-addresses* of the entry and the destination of a server operation. For host entries, this value will always be 0.0.0.0. Next to this column, you will see combinations of the following values: NET — The entry is a network entry. HOST — The entry is a host entry. FIXED — The server cannot change this entry based on information in an ICMP Routing Redirect message. VAR — The server can change this entry based on information in an ICMP Routing Redirect message.
Last Modified	The date and time the entry was created or last modified. An asterisk character (*) following the time indicates that the internet route was learned from an ICMP message from an Internet gateway.

SHOW/LIST/MONITOR SERVER IP SECURITY Privilege: N, P

Use these commands to view a list of all Internet security entries and the *port-list* for which each entries applies.

Privileges

Non-privileged users can use the SHOW and LIST SERVER IP SECURITY commands. Only users at privileged ports can use the MONITOR SERVER IP SECURITY command.

Syntax

```
SHOW/LIST/MONITOR SERVER IP SECURITY
```

Example

```
MX1620>> MONITOR SERVER IP SECURITY
Ports Set to Default Inbound Allow:    0-20
Ports Set to Default Inbound Deny:

Ports Set to Default Outbound Allow:   0-20
Ports Set to Default Outbound Deny:

      Internet        Security
Entry Address         Mask                  Access  Dir           Port(s)
1              192.12.119.206  255.255.0.0           Allow     Outbound     1,4,5

2              192.13.119.45   255.255.255.0         Allow     Inbound      0,9,16

3              192.11.110.40   255.255.255.255       Deny      Outbound     1-4,7
```

SHOW/MONITOR/LIST SERVER IP SECURITY DISPLAY

The following table describes each field on the LIST/MONITOR/SHOW SERVER IP SECURITY display

Field	Description
Ports Set to Default Inbound Allow	Shows which ports allow inbound connections to a connection partner when there is no entry in the Internet Security table for the connection partner.
Ports Set to Default Inbound Deny	Shows which ports deny inbound connections to a connection partner when there is no entry in the Internet Security table for the connection partner.
Ports Set to Default Outbound Allow	Shows which ports allow outbound connections to a connection partner when there is no entry in the Internet Security table for the connection partner.

SHOW/LIST/MONITOR SERVER IP SECURITY (continued)

Ports Set to Default Outbound Deny	Shows which ports deny outbound connections to a connection partner when there is no entry in the Internet Security table for the connection partner.
Entry	The number of the entry in the port's Internet Security table.
Internet Address	The target address of the destination.
Security Mask	Describes how to interpret the target address.
Access	Either Deny (prevent connection) or Allow (permit connection).
Dir	Either Inbound (from the network) or outbound (to the network).
Port(s)	The ports which are affected by the entry.

SHOW/LIST/MONITOR SERVER IP SNMP CHAR Privilege: See Below

Use these commands to display information about how SNMP clients are configured on the unit.

Privileges

Non-privileged users can use the SHOW and LIST SERVER IP SNMP CHAR commands. Only users at privileged ports can use the MONITOR SERVER IP SNMP CHAR command.

Syntax

SHOW/LIST/MONITOR SERVER IP SNMP CHARACTERISTICS

Example

```
Xyplex>> show server snmp char

MX1620 V6.0.4S10 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 1 19:08:48
Internet Address:  140.179.245.192       Subnet Mask:  255.255.128.0

System Name:           MINEALLMINE
System Location:       Littleton
System Contact:        Network Administrator

Authent. Traps:    Enabled
Get Community:     PUBLIC
Set Community:     PUBLIC
Trap Community:    PUBLIC

Get Client 1:                            Set Client 1:
Get Client 2:                            Set Client 2:
Get Client 3:                            Set Client 3:
Get Client 4:                            Set Client 4:
Get Client 5:                            Set Client 5:
Get Client 6:                            Set Client 6:
Get Client 7:                            Set Client 7:
Get Client 8:                            Set Client 8:
Get Client 9:                            Set Client 9:
Get Client 10:                           Set Client 10:
Get Client 11:                           Set Client 11:
Get Client 12:                           Set Client 12:

Trap Client 1:
Trap Client 2:
Trap Client 3:
Trap Client 4:
Trap Client 5:
Trap Client 6:
Trap Client 7:
Trap Client 8:
Trap Client 9:
Trap Client 10:
Trap Client 11:
Trap Client 12:
```

SHOW/LIST/MONITOR SERVER IP SNMP CHARACTERISTICS Display

SHOW/LIST/MONITOR SERVER IP SNMP CHARACTERISTICS (continued)

The following list describes the fields on the SHOW/LIST/MONITOR SERVER IP SNMP CHARACTERISTICS display:

Field	Description
Internet Address	The Internet address of the server.
Subnet Mask	The server's Subnet Mask.
System Name	The server *domain-name*, as defined via the DEFINE SERVER IP NAME command.
System Location	The location of the unit. This information is provided for administrative or informational purposes only.
System Contact	The name of a system contact for the unit. This information is provided for administrative or informational purposes only.
Authent. Traps	If enabled, the server is configured to generate authentication failure traps.
Get/Set/Trap Community	The name of the SNMP community to which the unit belongs. When a community name has been specified for the unit, only SNMP clients (e.g., a Network Operations Center, or NOC) which belong to the same community are permitted to obtain information from (i.e., perform an SNMP get) or set or trap characteristics (i.e., perform an SNMP set) on a unit.
Get/Set/Trap Client 1 - 12	The SNMP clients (e.g., a Network Operations Center, or NOC) which are permitted to set characteristics (i.e., perform an SNMP set) on the unit. Default: 0.0.0.0.

SHOW/MONITOR SERVER IP SNMP COUNTERS Privilege: See Below

Use these commands to view statistics about server SNMP activity and occurrences of error conditions.

Privileges

Non-privileged users can use the SHOW and LIST SERVER IP SNMP COUNTERS commands. Only users at privileged ports can use the MONITOR SERVER IP SNMP COUNTERS command.

Syntax

```
SHOW/MONITOR SERVER INTERNET SNMP COUNTERS
```

Example

```
Xyplex>> show server internet snmp counters

MX1620 V6.0.4S10 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 1 19:09:05
Internet Address:  140.179.245.192         Subnet Mask:  255.255.128.0

Packets Received:                210       Get Nexts Received:             126
Packets Transmitted:             210       Set Requests Received:            0
Version Errors:                    0       Too Big Errors:                   0
Community Name Errors:             0       No Such Name Errors:             28
Community Use Errors:              0       Bad Value Errors:                 0
ASN Parse Errors:                  0       Read Only Errors:                 0
Type Errors:                       0       General Errors:                   0
Requested Variables:             513       Get Responses Transmitted:      211
Set Variables:                     0       Traps Transmitted:                0
Get Requests Received:            85
```

SHOW/MONITOR SERVER IP SNMP COUNTERS Display

The following list describes the fields on the SHOW/MONITOR SERVER IP SNMP COUNTERS display:

SHOW/MONITOR SERVER IP SNMP COUNTERS (continued)

Field	Description
Packets Received	The number of SNMP packets the server has received.
Packets Transmitted	The number of SNMP packets the server has transmitted.
Version Errors	The number of syntactically correct SNMP packets received by the server, which were for an unsupported SNMP version.
Community Name Errors	The number of SNMP packets received by the server, which used an SNMP community name unknown to the server.
Community Use Errors	The number of SNMP packets received by the server, which represented an SNMP operation not allowed by the SNMP community named in the packet.
ASN Parse Errors	The number of ASN.1 parsing errors (either in encoding or syntax) the server encountered while decoding received SNMP packets.
Type Errors	The number of SNMP packets of unknown packet type that the server has received.
Requested Variables	The total number of Management Information Base (MIB) objects that have been retrieved from the server as the result of SNMP Get-Request and Get-Next packets the server received.
Set Variables	The number of MIB objects that have been altered as the result of valid SNMP Set-Request packets the server received.
Get Requests Received	The number of SNMP Get-Request packets that the server has received and processed.
Get Nexts Received	The number of SNMP Get-Next packets that the server has received and processed.
Set Requests Received	The number of SNMP Set-Request packets that the server has received and processed.

SHOW/MONITOR SERVER IP SNMP COUNTERS (continued)

Too Big Errors	The number of valid SNMP packets generated by the server, for which the value of the ErrorStatus component is "tooBig". (The server creates these packets in response to SNMP packets it receives that would generate a response that is too big.)
No Such Name Errors	The number of valid SNMP packets generated by the server, for which the value of the ErrorStatus component is "NoSuch Name". (The server generates these packets in response to SNMP packets it receives that contain an invalid object name.)
Bad Value Errors	The number of valid SNMP packets generated by the server, for which the value of the ErrorStatus component is "badValue". (The server generates these packets in response to SNMP packets it receives that contain an invalid value.)
Read Only Errors	The number of valid SNMP packets generated by the server, for which the value of the ErrorStatus component is "readOnly". (The server generates these packets in response to SNMP packets it receives that attempt to set a value that is read-only.)
General Errors	The number of valid SNMP packets generated by the server, for which the value of the ErrorStatus component is "genErr". (The server creates these packets in response to SNMP packets it receives that generate errors other than "tooBig", "NoSuchName", "badvalue", or "readOnly".)
Get Responses Transmitted	The number of SNMP Get-Response packets that the server has generated.
Traps Transmitted	The number of SNMP Trap packets that the server has generated.

SHOW/MONITOR SERVER IP TRANSLATION TABLE Privilege: See Below

Use this command to view information about the IP-address to Ethernet address mappings that it has learned. This is commonly referred to as the ARP table.

Privileges

Non-privileged users can use the SHOW SERVER IP TRANSLATION TABLE commands. Only users at privileged ports can use the MONITOR SERVER IP TRANSLATION TABLE command.

Syntax

```
SHOW/MONITOR SERVER IP TRANSLATION TABLE
```

Example

```
Xyplex>> SHOW SERVER IP TRANSLATION TABLE
MX1620 V6.0.4S10 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 1 19:09:28

Internet Address:  140.179.245.192
Domain Name:
Domain Suffix:



Table TTL: 60

Entry       Ethernet Address        IP Address      Receive TTL     Send TTL
1           08-00-20-78-8B-45      140.179.146.23       52              52
2           08-00-20-79-26-B4     140.179.162.204       52              52
3           08-00-20-72-32-74       140.179.248.1       52              52
4           00-20-AF-DA-F2-BF     140.179.240.183       59              59
5           00-80-F1-00-05-3F      140.179.162.63       52              52
6           08-00-20-0D-ED-BA       140.179.161.9       52              52
7           08-00-20-71-6D-00      140.179.146.22       52              52
8           08-00-87-4D-DF-97       140.179.131.2       60               2
9           08-00-20-1A-7B-A2      140.179.161.13       52              52
13          08-00-20-79-E7-41     140.179.248.177       52              52
14          08-00-20-0F-40-AC     140.179.162.171       52              52
23          00-20-AF-DA-F4-D0     140.179.176.102       60               1
36          08-00-20-1F-4C-95      140.179.162.99       52              52
43          08-00-20-72-97-28      140.179.240.80       52              23
91          08-00-09-78-26-93      140.179.252.43       52              52
181         08-00-20-08-8E-60       140.179.161.2       52              52
244         08-00-20-06-61-DD     140.179.130.201       52              52
```

SHOW/MONITOR SERVER IP TRANSLATION TABLE Display

SHOW/MONITOR SERVER IP TRANSLATION TABLE (continued)

The following list describes the fields on the SHOW/MONITOR SERVER IP TRANSLATION TABLE display

:

Field	Description
Internet Address	The Internet address of the server.
Domain Name	The Domain Name of the server.
Domain Suffix	The default Domain Name Suffix for the server.
Entry	The entry number assigned by the server for each Ethernet address/Internet address pair.
Ethernet Address	An Ethernet address that is mapped to a corresponding Internet address in the IP Address column.
IP Address	An Internet address that is mapped to a corresponding Ethernet address in the Ethernet Address column.
Receive TTL	The minutes remaining until the server discards the entry. This value is reset to its initial setting, 60 minutes, whenever the server receives a packet from the IP Address for the entry.
Send TTL	The minutes remaining until the server discards the entry. This value is reset to its initial setting, 60 minutes, whenever the server sends a packet to the IP Address for the entry.

SHOW/LIST/MONITOR SERVER KERBEROS Privilege: See Below

Use this command to view information about how the Kerberos security feature is configured on the unit.

Privileges

Non-privileged users can use the SHOW and LIST SERVER KERBEROS commands. Only users at privileged ports can use the MONITOR SERVERKERBEROS command.

Syntax

SHOW/LIST/MONITOR SERVER KERBEROS

Example

```
MX1620> SHOW SERVER KERBEROS
MX1620 V6.0.4S11 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 31 18:32:45
                                                  05 Oct 1998  12:09:14
Kerberos Security:         NONE           Kerberos Version 4
Kerberos Realm:
Kerberos Master:           NONE
Resolved Address:          0.0.0.0
Kerberos Primary Server:   NONE
Resolved Address:          0.0.0.0
Kerberos Secondary Server: NONE
Resolved Address:          0.0.0.0              739 Error Message:
Please contact your system administrator
Kerberos Port Number:      750      Kerberos Password Port:    749
Kerberos Query Limit:      3        Password Service: kadmin
Kerberos Ports Enabled:
Successful Logins:         0        Unsuccessful Logins:         0
Logins without Kerberos:   1        Password Change Failures:    0
Last Kerberos Error:       0        Occurred:

Attempts to access:        Master            Server1              Server2
Successful:                     0                 0                    0
Unsuccessful:                   0                 0                    0
```

SHOW/MONITOR/LIST SERVER KERBEROS Display

The following list describes the SHOW/MONITOR/LIST SERVER KERBEROS display fields: .

Field	Description
Kerberos Security	The value LOGIN indicates that the server provides Kerberos user verification. The value NONE indicates that the server does not provide Kerberos verification.
Kerberos Version	Either 4 or 5.
Kerberos Realm	The name of the Kerberos realm to which the Master and Server hosts are associated.
Kerberos Master	The Domain name and Internet address of the Kerberos Master host. The Kerberos Master maintains the Kerberos database and provides information to Server hosts within a realm. A server must query the Master when a user changes a Kerberos password.
Resolved Address	The "Resolved Address" field next to each Kerberos Server refers to the internet-address currently in use that maps to the domain-name.
Kerberos Primary Server	The Domain name and Internet address of the primary Server host. The primary Server host is the first Server host to be queried for user verification.
Kerberos Secondary Server	The Domain name and Internet address of the secondary Server host. The server queries the secondary Server host if the primary Server host does not respond.
Kerberos Port Number	The port number Kerberos is assigned to.
Kerberos Query Limit	The maximum number of queries the server can make when attempting to verify a Kerberos ID or change a password.
Kerberos Ports Enabled	The server ports for which Kerberos user verification has been enabled.
Successful Logins	The number of successful attempts to log on to a server port for which Kerberos user verification is enabled.

Logins without Kerberos

The number of logins that were made without Kerberos authentication.

Note: Kerberos may not be enabled on all ports.

Last Kerberos Error

Kerberos 4 or 5 Errors. .

The error number of the last Kerberos-related error to have occurred, and the date and time that it occurred. The following Kerberos errors can appear here:

Kerberos 4 Errors

1	Principal expired
2	Service expired
3	Authentication expired
4	Protocol version unknown
5	Wrong master key version
6	Wrong master key version
7	Byte order unknown
8	Principal unknown
9	Principal not unique
10	Principal has null key
20	Generic error from KDC
21	Can't read ticket file
22	Can't find ticket or TGT
26	TGT expired
31	Can't decode authenticator
32	Ticket expired
33	Ticket not yet valid
34	Repeated request
35	The ticket isn't for us
36	Request is inconsistent
37	delta_t too big
38	Incorrect net address
39	Protocol version mismatch
40	Invalid msg type
41	Message stream modified
42	Message out of order

Kerberos 4 Errors (continued)

.

43	Unauthorized request
51	Current PW is null
52	Incorrect current password
53	Protocol error
54	Error returned by KDC
55	Null tkt returned by KDC
56	Retry count exceeded
57	Can't send request
61	Not ALL tickets returned
62	Incorrect password
63	Protocol error
70	Other error
71	Don't have TGT
76	No ticket file found
77	Couldn't access tkt file
78	Couldn't lock ticket file
79	Bad ticket file format
80	tf_init not called first
81	Bad Kerberos name format
82	No Realm defined
83	Bad Service
84	Cannot allocate packet
7205	Time not within 5 minutes of server

Kerberos 5 Errors .

0	No error
1	Client's entry in database has expired
2	Server's entry in database has expired
3	Requested protocol version not supported
4	Client's key is encrypted in an old master key
5	Server's key is encrypted in an old master key
6	Client not found in Kerberos database
7	Server not found in Kerberos database
8	Principal has multiple entries in Kerberos database
9	Client or server has a null key
10	Ticket is ineligible for postdating
11	Requested effective lifetime is negative or too short
12	KDC policy rejects request
13	KDC can't fulfill requested option
14	KDC has no support for encryption type
15	KDC has no support for checksum type
16	KDC has no support for padata type
17	KDC has no support for transited type
18	Clients credentials have been revoked
19	Credentials for server have been revoked
20	TGT has been revoked
21	Client not yet valid - try again later
22	Server not yet valid - try again later
23	Password has expired
24	Preauthentication failed
25	Additional pre-authentication required
26	Requested server and ticket don't match
31	Decrypt integrity check failed
32	Ticket expired
33	Ticket not yet valid
34	Request is a replay
35	The ticket isn't for us
36	Ticket/authenticator don't match
37	Clock skew too great
38	Incorrect net

Kerberos Password Port	The port number that requires a Kerberos password for access.
Password Service	The name of the Kerberos password change service on the Kerberos master.

Unsuccessful Logins	The number of unsuccessful attempts to log on to a server port for which Kerberos user verification is enabled. (That is, the number of times a user entered an incorrect ID or password, and therefore could not log on to the port.) This value does not reflect unsuccessful attempts to query the Server hosts. .
Password Change Failures	The number of times a user attempted to change a Kerberos password but did not supply the required information. (The user did not enter the correct value at the "Old password:" prompt, or was unable to correctly verify the new password.) This value does not reflect unsuccessful attempts to query the Master hosts.
Occurred	When the last Kerberos error occurred.
Attempts to access	The number of successful and unsuccessful attempts by the server to access the Kerberos Master, Primary Server host (Server 1), and Secondary (Server 2) Server host.

LIST/MONITOR SERVER LOADDUMP CHARACTERISTICS Privilege: See Below

The LIST SERVER LOADDUMP CHARACTERISTICS command displays the initialization parameters in the initialization records you specify.

Privileges

Non-privileged users can use the LIST SERVER LOADDUMP CHARACTERISTICS command. Only users at privileged ports can use the MONITOR SERVER LOADDUMP CHARACTERISTICS command.

Syntax

LIST SERVER LOADDUMP [*record*/ALL] CHARACTERISTICS

Where	Means
[*record*]	One or more of the following initialization records: PRIMARY, SECONDARY, TERTIARY, or ALL. The PRIMARY initialization record is the default.

Example

```
Xyplex>> LIST SERVER LOADDUMP CHARACTERISTICS

MX1620 V6.0.4S10 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 1 19:10:28
Address:   08-00-87-03-34-6B   Name:   X03346B              Number:     0

Primary record: Enabled

Internet Address: 140.179.245.192
Internet Load Host: 140.179.240.183
Internet Load Gateway: 140.179.128.1
Internet Load File: xpcsrv20.sys
Internet Delimiter:  None

Software: XPCSRV20
Image Load Protocols Enabled: CARD, XMOP, MOP, BOOTP, RARP, DTFTP
Dump Protocols Enabled: XMOP, MOP, BOOTP, RARP
Parameter Load Protocols Enabled: NVS, BOOTP, RARP

Status Message: Enabled
Default Parameters: Disabled
```

LIST SERVER LOADDUMP CHARACTERISTICS (continued)

The following list explains the fields on the LOADUMP Characteristics display.

Primary Record	The status of the initialization record. This example The primary record enabled, but an initialization record can be enabled or disabled.
Internet Address	The Internet address of the access server.
Internet Load Host	The Internet address of the load host. Use the DEFINE SERVER LOAD IP HOST command to specify this information.
Internet Load Gateway	The Internet address of a gateway, if the access server requires a gateway to reach the Internet load host through DTFTP.
Internet Load File	The name and path of the software load image on the Internet host, that the access server loads through DTFTP.
Internet Delimiter	The file delimiter that the host should use during a DTFTP load.
Software	The CARD/XMOP/MOP software load image file name. Note: Xyplex Access Servers cannot load from a DEC Info Server or any other device that does not support loading via DEC MOP V3 using all 5 parameters (Including the fifth parameter, which is the Host date/time stamp) for "Parameter Load with Transfer Address" using MOP.
Image Load Protocols Enabled	The protocols that the initialization record can use to obtain the software load image.
Dump Protocols Enabled	The protocols that the initialization record can use to transmit a memory dump file.
Parameter Protocols Enabled	The protocols that the initialization record can use to obtain the parameter file.
Status Message	If enabled, status messages display during the loading process
Default Parameters	If enabled, the server will reboot using default parameters. If disabled (the default), the parameters are disabled with each reboot.

SHOW/MONITOR SERVER LPD COUNTERS Privilege: See Below

Use the SHOW/MONITOR SERVER LPD COUNTERS command to view statistical information about print jobs being handled by LPD queues that are enabled on the server. The SHOW command produces a "static" display of the requested information. These displays can be viewed on ANSI and non-ANSI terminals (including hardcopy devices). The MONITOR command generates a display that is continuously updated on the terminal display screen.

Privileges

Non-privileged users can use the SHOW SERVER LPD COUNTERS command. Only users at privileged ports can use the MONITOR SERVER LPD COUNTERS command.

Syntax

```
SHOW/MONITOR SERVER LPD COUNTERS
```

Example

```
Xyplex>> show server LPD counters
    LPD Queue      State   LF->LFCR   Total    Active    Waiting   Processed
----------------- -------- -------- --------- --------- --------- ------------
laser-printer     ENABLED  DISABLED         2         1         1          115
line-printer      DISABLED ENABLED          0         0         0           38
```

MONITOR/SHOW SERVER LPD COUNTERS Display

The following list explains fields on the MONITOR/SHOW SERVER LPD COUNTERS display.

SHOW/MONITOR SERVER LPD COUNTERS (continued)

Field	Description
LPD Queue	The name of an LPD queue (created and enabled/disabled using the DEFINE SERVER LPD QUEUE command).
State	Shows whether or not the LPD queue can accept job requests. Enabled means that the queue can accept job requests. Disabled means that the queue cannot accept job requests.
LF->LFCR	Shows whether or not the server will convert line-feed characters into carriage-return/line-feed characters. Enabled means that the server will make this conversion. Disabled means that the server will not make this conversion.
Total	The total number of jobs that are currently being processed by the LPD queue. The number shown equals the sum of the jobs shown in the "Active" and "Waiting" columns.
Active	The total number of jobs that are actively being printed at ports associated with the queue. (This number can be greater than 1 when the queue exists on more than one port.)
Waiting	The total number of jobs pending on the queue. The next job in the queue will be processed when a port associated with the queue becomes available.
Processed	The total number of jobs that the queue has previously completed.

SHOW/LIST/MONITOR SERVER LPD QUEUE Privilege: See Below

Use the SHOW/LIST/MONITOR SERVER LPD QUEUE command to view the status of all print jobs that are being processed by one or more LPD queues.

The SHOW and LIST commands produce a "static" display of the requested information. These displays can be viewed on ANSI and non-ANSI terminals (including hard-copy devices). The MONITOR command generates a display that is continuously updated on the terminal display screen.

To remove a specific job from an LPD queue, use the lprm or REMOVE QUEUE ENTRY command.

Privileges

Non-privileged users can use the SHOW/LIST SERVER LPD QUEUE commands. Only users at privileged ports can use the MONITOR SERVER LPD QUEUE command.

Syntax

```
SHOW/MONITOR/LIST SERVER LPD QUEUE      "queue-name"
                                        [ALL]
```

Where	Means
queue-name	The name of the LPD queue that you want to view. The name can be up to 16 characters long, and is case sensitive. Enclose the name in double-quotation marks.
ALL	View information about all LPD queues.

Example

```
MX1620>> SHOW SERVER LPD QUEUE "laser-printer"
```

```
Xyplex>> SHOW SERVER LPD QUEUE
LPD Queue      : laser-printer
Queue Port(s)  : 5, 6
Status         : ENABLED, ACTIVE
LF_>LFCR       : DISABLED
Bypass         : ENABLED

   Job Status        Remote Host     Job #      File Name      File Size   Port
----------------- ----------------- ------- ----------------- ------------ ----
PRINTING/Data     unixhost                1 report1                37651    5
PRINTING/Data     cadstation              2 schematic             223592    6
WAITING/Port      cadstation              3 schematic             111678    0
```

MONITOR/SHOW/LIST SERVER LPD QUEUE Display

The following table describes the fields on the MONITOR/ SHOW/LIST SERVER LPD QUEUE display.

Field	Description
LPD Queue	The name of an LPD queue (created and enabled/disabled using the DEFINE SERVER LPD QUEUE command).
Queue Ports	The ports associated with the LPD queue.
Status	Shows whether or not the LPD queue can accept job requests, and whether or not the queue is currently processing any jobs. Enabled means that the queue can accept job requests. Disabled means that the queue cannot accept job requests. Active means that the queue is currently processing print jobs.
LF->LFCR	Whether or not the server will convert line-feed characters into carriage-return/line-feed characters. Enabled means that the server will make this conversion. Disabled means that the server will not make this conversion.
Bypass	Only displays if the LPD Queue Bypass feature is enabled. The port will be bypassed if it is Xoffed (such as when the printer is out of paper).

Job Status	The current status of a job. Possible states are listed at the end of this table:
Remote Host	The name of the host which originated the LPD print job.
Job #	The position of the job within the LPD queue. Jobs are processed on a first-come-first serve basis by the next available port.
File Name	The name of the file being processed by the queue.
File Size	The size of the file (in bytes).
Port	The port assigned to print the job. A zero indicates that the job has not yet been assigned.

Job Status States

ABORTED	The print job was aborted (for example, by an lprm command, REMOVE QUEUE command, etc).
ABORTED/Flushing	The queue is discarding data received for an aborted print job.
ASSIGNED/Port	The queue has assigned a port to a print job.
COMPLETED	The print job is complete.
ERROR	An error occurred while the job was being transferred from the remote host to the server.
INITIALIZED	The print job was recently created.
PRINTING/Control	The queue is receiving (and discarding) an LPD print job control file.
PRINTING/Data	The queue is receiving an LPD print job and sending it to the assigned port.
WAITING/Port	The print job is on the LPD print queue and is waiting for a port assignment.

SHOW/MONITOR SERVER LPD STATUS Privilege: See Below

Use these commands to view summary information about LPD queue availability. The SHOW command produces a "static" display of the requested information. These displays can be viewed on ANSI and non-ANSI terminals (including hardcopy devices). The MONITOR command generates a display that is continuously updated on the terminal display screen.

Privileges

Non-privileged users can use the SHOW SERVER LPD STATUS command. Only users at privileged ports can use the MONITOR SERVER LPD STATUS command.

Syntax

```
SHOW/MONITOR SERVER LPD STATUS
```

Example

```
Xyplex>> show server LPD status
    LPD Queue      State      LF->LFCR       Formfeed       Ports
----------------- --------    --------       --------       ----------------------------------
laser-printer     ENABLED     DISABLED       BEFORE         5-8
line-printer      DISABLED     ENABLED                      9-10
```

MONITOR/SHOW SERVER LPD STATUS Display

The following table describes each field on the MONITOR/SHOW SERVER LPD STATUS display.

Field	Description
LPD Queue	The name of an LPD queue (created and enabled/disabled using the DEFINE SERVER LPD QUEUE command).
State	Shows whether or not the LPD queue can accept job requests. Enabled means that the queue can accept job requests. Disabled means that the queue cannot accept job requests.
LF->LFCR	Shows whether or not the server will convert line-feed characters into carriage-return/line-feed characters. Enabled means that the server will make this conversion. Disabled means that the server will not make this conversion.
Formfeed	If enabled, shows whether the LPD queue will add a formfeed before, after or no formfeed to the print job.
Ports	The ports associated with the LPD queue.

SHOW/LIST/MONITOR SERVER MENU Privilege: P

Use the SHOW/LIST/MONITOR SERVER MENU display to view a list of all menu entries stored in the operational or permanent database. The output of these commands includes the menu items and the corresponding TCP/IP-LAT or access server commands. See the *Advanced Configuration Guide* for a description of the Simple Menu Interface feature.

Syntax

```
SHOW/LIST/MONITOR SERVER MENU
```

Example

```
Xyplex>> SHOW SERVER MENU

1.              Show Characteristics
                SHOW PORT CHARACTERISTICS; SHOW PORT ALT CHAR
2.
.
.
.
9.              Support
                CONNECT SYSTEM_SUPPORT

10.

11.Connect
                TELNET CONNECT 192.12.119.74
.
.
.
20.

Menu Prompt: Enter number of selection or use arrow keys:
Menu Continue Prompt: press <RETURN> to continue...
```

Example SHOW/LIST SERVER MENU Display

For each entry shown in the SHOW/LIST SERVER MENU display, the server displays the command shown on the menu to users who are logged on to ports for which the menu interface is enabled. The second line of the entry displays the corresponding Xyplex LAT-TCP/IP command for the menu item.

SHOW/LIST/MONITOR SERVER RADIUS Privilege: N, P

Use this command to display the RADIUS authentication feature on your access server.

Note: If the following error message displays when you use this command, this means that Radius is disabled on the server.

```
786 - Resolve Service and Preferred/Dedicated Service Conflict
```

Use the DEFINE SERVER RADIUS ENABLED to enable Radius on the server.

Syntax

```
SHOW/LIST/MONITOR SERVER RADIUS
```

Example

```
Xyplex> SHOW SERVER RADIUS
MX1620 V6.0.4S11 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 31 20:11:33
                                                  05 Oct 1998  13:48:02

Radius Primary Server:     140.179.248.145
Resolved Address:           140.179.248.145    Secret:  CONFIGURED

Radius Secondary Server:   NONE
Resolved Address:          0.0.0.0            Secret:  DEFAULT

Radius Port Number:        1645               Request Timeout (sec):    131
Radius Logging:            ENABLED            Chap Challenge Size:      16
Radius Server Retries:     3
Radius Ports Enabled:

Successful Logins:         0                  Configuration Failures:   0
Authentication Failures:   0                  Policy Failures:          0

Total Authentication and Accounting Server attempts:
                              Primary           Secondary
   Successful attempts:          4                 0
   Failed attempts:              0                 0
```

The following list describes the fields on the SHOW SERVER RADIUS screen:

Field	Description
Radius Primary Server	The first Radius server tried for each authentication attempt.
(Primary) Resolved Address	When the Radius primary server is specified as a DNS name, the name must be resolved to an IP address. The resolved address for the Primary Server appears here.
(Primary) Secret	Displays as DEFAULT when the primary server secret is not configured; the word CONFIGURED displays otherwise.

SHOW/LIST/MONITOR SERVER RADIUS (continued)

Radius Secondary Server	Specifies the DNS name of the Radius server tried after the Primary Server is tried. The default value is the null string "".	
(Secondary) Resolved Address	Specifies the resolved address of the Radius server queried for user verification if the primary server does not respond. The default value is 0.0.0.0.	
(Secondary) Secret	Shows if the secondary server secret is configured or not (if it is not configured , the value appears as DEFAULT).	
Radius Port Number	The UDP port on which Radius user verification requests are transmitted and received.	
Radius Logging	This controls whether the Radius client logs messages to the accounting log. The default is Disabled.	
Radius Server Retries	The number of times connection will be attempted.	
Radius Ports Enabled	A bitmask indicating which ports on the server have Radius enabled for either interactive or PPP use.	
Request Timeout	The period between Radius client retransmissions to the server when trying to authenticate a user. The default value is 5 seconds.	
Chap Challenge Size	The number of characters configured for the Chap challenge size. Note that current Radius servers only support a Chap challenge string length of 16 characters.	
Successful Logins	The number of successful logins using Radius	
Authentication Failures	The number of unsuccessful logins using Radius.	
Configuration Failures	The number of login failures that occurred due to configuration failures.	
Policy Failures	The number of login failures that occurred due to policy failures.	
Total Authentication and Accounting Server Attempts	Successful attempts	The number of times the primary/secondary Radius server and the client successfully exchanged messages
	Failed attempts	The number of times the primary/secondary Radius server and the client failed to exchange messages.

SHOW/LIST/MONITOR SERVER SCRIPT SERVER Privilege: See Below

Use these commands to view a list of all script servers (i.e., hosts that can download a script file to this server). See the *Advanced Configuration Guide* for a description of the Network Scripts feature.

Privileges

Non-privileged users can use the SHOW/LIST SERVER SCRIPT SERVER commands. Only users at privileged ports can use the MONITOR SERVER SCRIPT SERVER command.

Syntax

```
SHOW/LIST/MONITOR SERVER SCRIPT SERVER
```

Example

```
MX1620 V6.0.4S11 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 31 20:23:06
Address:   08-00-87-03-34-6B   Name:   X03346B              Number:     0

Script Servers:

Entry 1: 140.179.240.183 scripts  /


MX1620>
```

SHOW/MONITOR/LIST SERVER SCRIPT SERVER Display

For each entry shown in the SHOW/LIST SERVER SCRIPT SERVER display, the server shows the IP address or domain-name of the script server, and the directory path at the script server where it will search for script files and the file delimiter.

SHOW/LIST/MONITOR SERVER SECURID Privilege: See Below

Use the SHOW/LIST/MONITOR SERVER SECURID command to view the current SecurID-related settings, as well as information about successful and unsuccessful authentication attempts and logins using SecurID.

See the Using Security Feature chapter in the *Advanced Configuration Guide* for more information about setting up SecurID.

Privileges

Non-privileged users can use the SHOW/LIST SERVER SECURID commands. Only users at privileged ports can use the MONITOR SERVER SECURID command.

Syntax

```
SHOW/LIST/MONITOR SERVER SECURID
```

Example

```
MX1620> SHOW SERVER SECURID

MX1620 V6.0.4S11 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 31 20:36:40
                                                  05 Oct 1998  14:13:09

SecurID Server0: SECURID_0                  Resolved Address:     140.179.159.1
SecurID Server1: SECURID_1                  Resolved Address:     140.179.136.20
SecurID Server2: NONE                       Resolved Address:           0.0.0.0
SecurID Server3: NONE                       Resolved Address:           0.0.0.0
SecurID Server4: NONE                       Resolved Address:           0.0.0.0
SecurID ACMMAXRETRIES:     5                SecurID ACMBASETIMEOUT:           3
SecurID ACM_PORT:          755              SecurID Query Limit:              3
SecurID Encryption Mode:   DES

SecurID Ports Enabled: 1,3

Successful Logins:         1                Last Unsuccessful Login:       Port_3
Logins without SecurID:    42
Unsuccessful Logins:       0

Attempts to access:  Server0      Server1      Server2      Server3     Server4
Successful:                0            0            0            0           0
Unsuccessful:              0            0            0            0           0

MX1620>>
```

SHOW/LIST/MONITOR SERVER SECURID (continued)

The following table describes each field on the MONITOR/SHOW/ LIST SERVER SECURID display:

Field	Description
SecurID Server0 through SecurID Server 4	The domain-name of any primary or secondary ACE/Server hosts that have been defined. The "Resolved Address" field next to each SecurID Server refers to the internet-address currently in use that maps to the domain-name. .
SecurID AMCMAXRETRIES	The number of times that the Xyplex client will attempt to connect to the ACE/Servers in its list of ACE/Servers in order to authenticate a user.
SecurID ACM_PORT	The destination UDP port number to use when sending information to one or more ACE/Servers in order to authenticate a user.
SecurID Encryption Mode	The type of encryption that is used by the SecurID client when it communicates with an ACEserver.
Resolved Address (Server0-Server4)	The "Resolved Address" field next to each SecurID Server refers to the internet-address currently in use that maps to the domain-name.
SecurID ACMBASETIMEOUT	The initial time between prompts for a PASSCODE.
SecurID Query Limit	The number of times that a user at a Xyplex client can enter a PASSCODE before the Xyplex unit will log out the port.
SecurID Ports Enabled	The ports which require that the SecurID host authenticate the user when he or she attempts to log in.

The following fields are not shown in LIST command displays:

Field	Description
Successful Logins	The number of times that users were successfully authenticated and logged on to the server.
Logins without SecurID	The number of times users logged on to ports at which SecurID is not enabled.
Unsuccessful Logins	The number of times that users attempted to log on to the server, but were unsuccessful at passing SecurID authentication.
Last Unsuccessful Login	The name of the last port at which user was not able to be authenticated and logged on. If there have been no unsuccessful login attempts, the display will say "None."
Attempts to access: Server0 through Server4	The number of times that the client attempted to access a primary or alternate ACE/Servers to authenticate a user. When the client received a response from a given ACE/Server, it is listed as a successful attempt to access that ACE/Server. When the client did not receive a response from a given ACE/Server, it is listed as an unsuccessful attempt to access that ACE/Server.

SHOW/MONITOR SERVER STATUS Privilege: See Below

Use these commands to view detailed information about the current, highest (since server initialization), and permitted maximum levels of port activity, service activity, connection activity, and server resources that can be used, as well as some cumulative errors that have occurred since the server was last initialized.

Privileges

Non-privileged users can use the SHOW SERVER STATUS commands. Only users at privileged ports can use the MONITOR SERVER STATUS command.

Syntax

```
SHOW/MONITOR SERVER STATUS
```

Example

```
MX1620 V6.0.4S11 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 31 20:50:35
Address:   08-00-87-03-34-6B   Name:   X03346B              Number:     0

                      Cur  High  Max

Active Port settings:          2     2   21     Minutes To Shutdown:        N/A
Active Users:           2     2   21     Discarded Nodes:              0
Queue Entries:          0     0   24     Resource Errors:              0

Available Services:    30    36  N/A     Port Framing Errors:         39
Local Services:         1     1   24     Port Parity Errors:           0
Reachable Nodes:       13    15  100     Port Overrun Errors:          0

Active Circuits:        0     0   40     Primary Hosts:
Connected Nodes:        0     0   40     Load Address: 08-00-87-03-34-6B
Connected Sessions:     1     2   64     Dump Address: 08-00-87-03-34-6B
% CPU Used:            11   100  100     Console User:   140.179.133.136
% Memory Used:          3     5  100     Nested Menu Memory:           0

Selftest Status:  Normal
Software Status:  Normal
```

SHOW SERVER STATUS Display

SHOW/MONITOR SERVER STATUS (continued)

This display shows the server's current status, and may be helpful in identifying network trouble or port problems. For each server resource listed, the display shows the following information.

Cur — the level or amount of the resource that is currently in use. (Note that if the maximum value for the resource was changed since the last time the counters were reset to zero, the value in this column may exceed the value in the Max column.)

High — the highest amount of the resource that has been used since the server was last initialized. (Note that if the maximum value for the resource was changed since the last time the server was re-initialized, the value in this column may exceed the value in the Max column.)

Max — the maximum amount of the resource that can be used (either because of a hardware constraint or because the value shown is the value specified for a server setting).

The following table describes each field on the LIST/MONITOR/SHOW SERVER STATUS display after the header lines:

Field	Description
Active Ports	The number of ports that have interactive sessions or remote-access connections.
Active Users	The number of ports that have interactive sessions connected.
Queue Entries	The number of connection requests that are queued in the server connection queue
Available Services	The number of LAT services about which the server has retained information in its memory, and are therefore available to users.
Local Services	The number of LAT services offered at the server.
Reachable Nodes	The number of LAT nodes (computers, other servers, etc) that offer services and are reachable for service connections.
Active Circuits	The number of LAT virtual circuits on which the server has active connections with service nodes.
Connected Nodes	The number of service nodes with which the server has an established LAT virtual circuit.

Connected Sessions	The total number of sessions which the server has currently connected.
% CPU Used	The percentage of processing time that the server has used (calculated every second).
% Memory Used	The percentage of the server memory pool that is being used to store information for the node and service database, queued requests, and multiple-service sessions.
Minutes To Shutdown	The number of minutes remaining until the server re-initializes (or N/A if no INITIALIZE command has been issued).
Discarded Nodes	The number of nodes that could not be included in the server node database because the value set for the SERVER NODE LIMIT characteristic has been reached or because of insufficient memory.
Resource Errors	The number of times that insufficient server memory prevented the creation of an internal data structure.
Port Framing Errors	The total number of bytes received at all ports which had illegally formatted data characters.
Port Parity Errors	The total number of bytes received at all ports which had parity errors.
Port Overrun Errors	The total number of times that bytes were lost at any port because the server input buffers were full.
Primary Hosts	The names of the hosts from which the server was last loaded.

Load Address	The Ethernet address or *internet-address* of the host from which the server was last loaded.
Dump Address	The Ethernet address or *internet-address* of the node that received the last server memory dump.
Console User	The Ethernet address of a remote device at which a user has initiated a session with the console port of this server.

SHOW/MONITOR SERVER STATUS (continued)

Nested Menu Memory	The amount of memory allocated for the nested menu.
Selftest Status	Always Normal (you would not be able to see this display otherwise).
Software Status	Always Normal (you would not be able to see this display otherwise).

SHOW/LIST/MONITOR SERVER SUMMARY Privilege: See Below

Use these commands to view a summary showing the identity of the server and the total list of authorized LAT groups defined at this server.

Privileges

Non-privileged users can use the SHOW/LIST SERVER SUMMARY commands. Only users at privileged ports can use the MONITOR SERVERSUMMARY command.

Syntax

```
SHOW/LIST/MONITOR SERVER SUMMARY
```

Example

```
Xyplex>> show server summary

MX1620 V6.0.4S10 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 1 19:14:08
Address:   08-00-87-03-34-6B   Name:   X03346B              Number:     0

Identification:  Xyplex Access Server

Server Groups: 0-7, 100-110
```

LIST/MONITOR/SHOW SERVER SUMMARY Display

The following table describes each field on the display.

Field	Description
Identification	Shows a text message which identifies the server.
Server Group	The authorized LAT groups that can have access to this server.

SHOW/LIST SERVER TN3270 Privilege: N, P

Use this command to view the names of TN3270 devices and translation tables on this server, and whether port keymaps is enabled or disabled. Refer to the *Advanced Configuration Guide* for a description of the TN3270 feature.

Syntax

```
SHOW/LIST SERVER TN3270
```

Example

```
MX1620> SHOW SERVER TN3270

MX1620 V6.0.4S11 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 31 22:13:37
Address:   08-00-87-03-34-6B   Name:   X03346B              Number:     0


Port Keymaps : Enabled

Devices : ANSI, VT100, VT220-7, VT220-8

TranslationTables : USENGLSH


MX1620>
```

SHOW/LIST SERVER TN3270 Display

The following table describes the fields on the LIST/SHOW SERVER TN3270 display:

Field	Description
Port Keymaps	Indicates whether or not SERVER TN3270 PORT KEYMAPS is enabled or disabled on this server. This characteristic controls whether or not individual ports can maintain their own copies of keymaps.
Devices	Lists the TN3270 device types available on this server. See the DEFINE/SET SERVER TN3270 for more information.
Translation Tables	Lists the TN3270 translation tables available on this server. See the DEFINE/SET SERVER TN3270 for more information.

SHOW/LIST SERVER TN3270 DEVICE Privilege: N, P

Use the SHOW/LIST SERVER TN3270 DEVICE command to view information about the TN3270 devices. See the *Advanced Configuration Guide* for a description of the TN3270 feature.

Syntax

SHOW/LIST SERVER TN3270 DEVICE *device-name*

Where	Means
device-name	The server will display information about the device you specify, such as the TN3270 type, the Model type, and the keymap and screenmap escape sequences.

Example

```
Xyplex>> SHOW SERVER TN3270 DEVICE VT100
MX1620 V6.0.4S10 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 0 01:01:15
Address:   08-00-87-03-34-6B   Name:   X03346B             Number:     0
Device: VT100       TerminalType: VT100                  Tn3278Type : MODEL2

Keymap:
3270-Key         Description  KeyCode

NEWLINE       :  LF           "0A"
TAB           :  TAB          "09"
BACKTAB       :  ESCTB        "1B 09"
UP            :  KEYUP        "1B 5B 41"
LEFT          :  KEYBK        "1B 5B 44"
RIGHT         :  KEYFW        "1B 5B 43"
DOWN          :  KEYDN        "1B 5B 42"
HOME          :  ESCh         "1B 68"
DELETE        :  DEL          "7F"
ERASEEOF      :  CTRLe        "05"
ERASEINP      :  ESCi         "1B 69"
INSERT        :  ESCDL        "1B 7F"
FLUSHINP      :  ESCf         "1B 66"
REFRESH       :  ESCr         "1B 72"
CENTSIGN      :  ESCc         "1B 63"
DUPLICAT      :  CTRLd        "04"
FIELDMRK      :  CTRLf        "06"
SCROLL        :  ESCl         "1B 6C"
STATUS        :  ESC?         "1B 3F"
RESET         :  CTRLr        "12"
FASTLEFT      :  CTRLv        "16"
FASTRGHT      :  CTRLu        "15"
SHOWKEYS      :  CTRLx        "18"
PRINT         :  CTRLp        "10"
PF1           :  NUM 1        "1B 4F 71"
PF2           :  NUM 2        "1B 4F 72"
PF3           :  NUM 3        "1B 4F 73"
PF4           :  NUM 4        "1B 4F 74"
PF5           :  NUM 5        "1B 4F 75"
PF6           :  NUM 6        "1B 4F 76"
PF7           :  NUM 7        "1B 4F 77"
PF8           :  NUM 8        "1B 4F 78"
PF9           :  NUM 9        "1B 4F 79"
PF10          :  PF1          "1B 4F 50"
```

```
PF11          :  PF2          "1B 4F 51"
PF12          :  PF3          "1B 4F 52"
PF13          :  ESC!         "1B 21"
PF14          :  ESC@         "1B 40"
PF15          :  ESC#         "1B 23"
PF16          :  ESC$         "1B 24"
PF17          :  ESC%         "1B 25"
PF18          :  ESC^         "1B 5E"
PF19          :  ESC&         "1B 26"
PF20          :  ESC*         "1B 2A"
PF21          :  ESC(         "1B 28"
PF22          :  ESC)         "1B 29"
PF23          :  ESC_         "1B 5F"
PF24          :  ESC+         "1B 2B"
PA1           :  ESC,         "1B 2C"
PA2           :  ESC.         "1B 2E"
PA3           :  ESC/         "1B 2F"
SYSREQ        :  ESCs         "1B 73"
ENTER         :  ENTER        "0D"
CLEAR         :  CTRLc        "03"
CURSSEL       :  ESCk         "1B 6B"
TEST          :  ESCt         "1B 74"
```

SHOW/LIST SERVER TN3270 DEVICE Display

The following table describes the fields on the SHOW/LIST SERVER TN3270 DEVICE display:

Field	Description
Device	The name of the TN3270 device in the display.
TerminalType	The local terminal type.
Tn3278Type	The TN3270 device model that the local terminal emulates during a Tn3270 session.
Keymap	The table that follows contains the escape sequences that the access server uses to translate entries on the local ASCII keyboard into 3270 display station functions.
3270-Key	An IBM display station function.
Description	A text description of the keyboard function.
KeyCode	The hexadecimal value for the keyboard escape sequence at the local terminal which corresponds to the IBM display station function.

ScreenMap	The table that follows contains the escape sequences that the access server sends to the local terminal to initiate screen functions such as clear the screen, move the cursor, or set the bold attribute.
Terminal Function	The IBM screen function that occurs on the local terminal when the user enters the escape sequence indicated by the corresponding the Hex Code
Hex Code	The hexadecimal value of the escape sequence for the IBM terminal function.

SHOW/LIST SERVER TN3270 TRANSLATIONTABLE Privilege: N, P

Use the SHOW/LIST SERVER TN3270 TRANSLATIONTABLE display to view information in the EBCDICTOASCII or ASCIITOEBCDIC portion of the translation table you specify.

Syntax

SHOW/LIST SERVER TN3270 TRANSLATIONTABLE [*trans-name table]*

Where	Means
trans-name	The name of the translation table that will display information.
table	Which portion of the translation table the server will display. The valid values are ASCIITOEBCDIC or EBCDICTOASCII.

Example

```
MX1620 V6.0.4S10 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 0 01:02:35
Address:   08-00-87-03-34-6B   Name:   X03346B              Number:     0

TranslationTable Name: USENGLSH               Table: ASCIITOEBCDIC

     0x  1x  2x  3x  4x  5x  6x  7x  8x  9x  ax  bx  cx  dx  ex  fx
     ---------------------------------------------------------------
x0 | 00  00  40  f0  7c  d7  79  97  00  00  00  00  00  00  00  00
x1 | 00  00  5a  f1  c1  d8  81  98  00  00  00  00  00  00  00  00
x2 | 00  00  7f  f2  c2  d9  82  99  00  00  00  00  00  00  00  00
x3 | 00  00  7b  f3  c3  e2  83  a2  00  00  00  00  00  00  00  00
x4 | 00  00  5b  f4  c4  e3  84  a3  00  00  00  00  00  00  00  00
x5 | 00  00  6c  f5  c5  e4  85  a4  00  00  00  00  00  00  00  00
x6 | 00  00  50  f6  c6  e5  86  a5  00  00  00  00  00  00  00  00
x7 | 00  00  7d  f7  c7  e6  87  a6  00  00  00  00  00  00  00  00
x8 | 00  00  4d  f8  c8  e7  88  a7  00  00  00  00  00  00  00  00
x9 | 00  00  5d  f9  c9  e8  89  a8  00  00  00  00  00  00  00  00
xa | 00  00  5c  7a  d1  e9  91  a9  00  00  00  00  00  00  00  00
xb | 00  00  4e  5e  d2  4a  92  c0  00  00  00  00  00  00  00  00
xc | 00  00  6b  4c  d3  e0  93  6a  00  00  00  00  00  00  00  00
xd | 00  00  60  7e  d4  5a  94  d0  00  00  00  00  00  00  00  00
xe | 00  00  4b  6e  d5  5f  95  a1  00  00  00  00  00  00  00  00
xf | 00  00  61  6f  d6  6d  96  00  00  00  00  00  00  00  00  00
```

SHOW/LIST SERVER TN3270 TRANSLATION TABLE ASCIITOEBCDIC Display

SHOW/LIST SERVER TN3270 TRANSLATIONTABLE (continued)

```
MX1620 V6.0.4S10 Rom 470000 HW 00.00.00 Lat Protocol V5.2 Uptime: 0 01:03:22
Address:   08-00-87-03-34-6B   Name:   X03346B              Number:     0

TranslationTable Name: USENGLSH                Table: EBCDICTOASCII

     0x  1x  2x  3x  4x  5x  6x  7x  8x  9x  ax  bx  cx  dx  ex  fx
     ------------------------------------------------------------
x0 | 20  20  20  20  20  26  2d  20  20  20  20  20  7b  7d  5c  30
x1 | 20  20  20  20  20  20  2f  20  61  6a  7e  20  41  4a  20  31
x2 | 20  20  20  20  20  20  20  20  62  6b  73  20  42  4b  53  32
x3 | 20  20  20  20  20  20  20  20  63  6c  74  20  43  4c  54  33
x4 | 20  20  20  20  20  20  20  20  64  6d  75  20  44  4d  55  34
x5 | 20  20  20  20  20  20  20  20  65  6e  76  20  45  4e  56  35
x6 | 20  20  20  20  20  20  20  20  66  6f  77  20  46  4f  57  36
x7 | 20  20  20  20  20  20  20  20  67  70  78  20  47  50  58  37
x8 | 20  20  20  20  20  20  20  20  68  71  79  20  48  51  59  38
x9 | 20  20  20  20  20  20  20  60  69  72  7a  20  49  52  5a  39
xa | 20  20  20  20  5b  21  7c  3a  20  20  20  20  20  20  20  20
xb | 20  20  20  20  2e  24  2c  23  20  20  20  20  20  20  20  20
xc | 20  20  20  20  3c  2a  25  40  20  20  20  20  20  20  20  20
xd | 20  20  20  20  28  29  5f  27  20  20  20  20  20  20  20  20
xe | 20  20  20  2a  2b  3b  3e  3d  20  20  20  20  20  20  20  20
xf | 20  20  20  3b  7c  5e  3f  22  20  20  20  20  20  20  20  20
```

SHOW/LIST SERVER TN3270 TRANSLATIONTABLE EBCDICTOASCII Display

Field	Description
TranslationTable Name	The name of TN3270 language translation table.
Table	The portion of the translation table in the display. This can be the ASCIITOEBCDIC portion or the EBCDICTOASCII portion.

SHOW/LIST/MONITOR SERVER XREMOTE Privilege: N, P

Use the SHOW/LIST/MONITOR SERVER XREMOTE commands to display the current Xremote settings on the access server, including the primary and secondary font servers.

Syntax

```
SHOW/LIST/MONITOR SERVER XREMOTE
```

Example

```
Xyplex>> SHOW SERVER XREMOTE
 Address:      08-00-87-00-4F-4F      Name:   X004F4F Number:

 Xremote       Primary Font Server:   HOST.EAST.COM
                                      Address:                      130.124.80.112

 Xremote       Secondary Font Server: HOST.WEST.COM
                                      Address:                      130.124.80.112

 Xremote Ports Enabled        3, 4, 5
 Current Number of Xremote Sessions: 3       Current Number of Xclients: 3

 Attempts to access                                 Server1 Server2
 Successful    2              1
 Unsuccessful  0              1
```

Show/List/Monitor Server Xremote Display

Field	Description
Xremote Primary Font Server	The domain name of the primary font server.
Address	The Internet address of the primary font server.
Xremote Secondary Font Server	The domain name of the secondary font server.
Address	The Internet address of the secondary font server.
Xremote Ports Enabled	The ports on the access server that have Xremote enabled.

Current Number of Xremote Sessions	The number of Xremote sessions currently established at the ports with Xremote enabled. There is one Xremote session per active Xremote port. XREMOTE
Current Number of Xclients	The total number of Xclient processes on all ports of the access server. This value reflects the number of open X windows, one XDM manager and one window manager for each port with Xremote enabled.
Attempts to access	The number of successful and unsuccessful attempts to reach the primary font server and the secondary font server, if you have defined them.

SHOW/LIST/MONITOR SERVICES CHARACTERISTICS Privilege: See Below

Use this command to view the current settings that were defined using SET/DEFINE SERVICE commands).

Privileges

Secure and non-privileged users can use the SHOW and LIST SERVICES CHARACTERISTICS command, unless the DEFINE/SET PORT LIMITED VIEW characteristics is ENABLED. Only users at privileged ports can use the MONITOR SERVICES CHARACTERISTICS command.

Syntax

```
SHOW/MONITOR SERVICE    [service-name]    [CHARACTERISTICS]
                        [LOCAL]           [CHARACTERISTICS]
                        [ALL]             [CHARACTERISTICS]
LIST SERVICE            [service-name]    [CHARACTERISTICS]
                        [LOCAL]           [CHARACTERISTICS]
```

Where Means

service-name Specifies that the access server will display the requested information about one or more specific services that are available on the network to the user at the port where the request is made.

You can specify a wildcard character to select a subset of the *service-names* to be displayed. The asterisk symbol (*) is the wildcard character. For example, if one types SHOW SERVICES AB*, the server will display all accessible *service-names* whose names start with AB. SHOW SERVICES A*BC displays accessible *service-names* whose names start with A and end with BC.

ALL Specifies that the access server will display the requested information about all services that are available on the network to the user at the port where the request is made.

LOCAL Specifies that the access server will display the requested information about all services that are available locally on the access server to the user at the port where the request is made.

Example

```
Xyplex>> show services char

Service: 1C323                                        08 Oct 1998  09:12:40

Identification:

Service: 1C325                                        08 Oct 1998  09:12:40

Identification:
```

LIST/MONITOR/SHOW SERVICES CHARACTERISTICS Display

The following table describes the fields on the LIST/MONITOR/SHOW SERVICES CHARACTERISTICS display:

Field	Description
Service	The name of a service available on the network.).
Identification	A text string that identifies the service or describes how to use the service.
Enabled Characteristics	The settings that have been enabled for the local service(s) using DEFINE/SET SERVICE commands. Services only display if they have been enabled. The possible values are:
	Rating — The relative availability of the service. If there are any available ports which offer the service, then the rating shown is proportional to the number of available ports. If there are no available ports that offer the service, then the rating shown is zero (0).
	The following enabled characteristics on display on local services.
	Ports — The port numbers on the access server where locally offered services are available.
	Connections — Shows that the server allows connections to the service.

Password	Show that the server requires the requester of the service to provide a password, specified by the access server manager, before the service permits access to the service.).
Queuing	Shows that the server will place connection requests that cannot be satisfied immediately into a connection queue.

Example:

```
Service: FORUM                                                  18 Oct 1998  09:14:38
Identification: "Lab Printer"
Port settings: 4
Rating: 255
Enabled Characteristics:
Connections, Queuing, Password
```

In this example, a service called "FORUM' was defined on port 4 with an identification string of "Lab Printer." The Rating is the computed value of availability (this is not defined or set).

SHOW/MONITOR SERVICES STATUS Privilege: See Below

Use the SHOW/MONITOR SERVICES STATUS display to view detailed information about the operational condition and availability of services that are available on the network and/or locally available on the access server.

Privileges

Secure and non-privileged users can use the SHOW SERVICES STATUS command, unless the DEFINE/SET PORT LIMITED VIEW characteristics is ENABLED. Only users at privileged ports can use the MONITOR SERVICES STATUS command.

Syntax

```
SHOW/MONITOR SERVICE [service-name]    STATUS      [Local]
                                                   [ALL]
```

Where	Means
service-name	The access server will display the requested information about one or more specific services that are available on the network to the user at the port where the request is made. You can specify a wildcard character to select a subset of the *service-names* to be displayed. The asterisk symbol (*) is the wildcard character. For example, if one types SHOW SERVICES AB*, the server will display all accessible *service-names* whose names start with AB. SHOW SERVICES A*BC displays accessible *service-names* whose names start with A and end with BC.
ALL	The access server will display the requested information about all services that are available on the network to the user at the port where the request is made.
LOCAL	The access server will display the requested information about all services that are available locally on the access server to the user at the port where the request is made.

Example

```
Xyplex> SHOW SERVICE STATUS
 Service PRINTER -    Available
 Node Name           Status   Rating  Identification
 Service LASER -     Available
 Node Name           Status   Rating  Identification
 MAX5000             Reachable   127  Shared Laser Printer
 Service FINANCEVAX - Available
 Node Name           Status   Rating  Identification
 FINANCEVAX        5 Connected   72  Corporate MicroVAX II
```

MONITOR/SHOW SERVICES STATUS Display

The following table describes each field on the MONITOR/SHOW SERVICES STATUS display.

Field	Description
Service	The name of a service available on the network.
Node Name	The name of the node where the service is offered.
Status	Shows whether or not the service is currently reachable or available. The possible values which can be shown include:
	Available — At least one service node that offers the service has the status REACHABLE.
	n Connected — The service is reachable and the server has *n* currently active sessions with this service.
	Reachable — The service is reachable and the server has no currently active sessions with the service.
	Unknown — The service was available but now may be unavailable. This could be because the server has not recently received a multicast announcement from the service node(s) which offer(s) the service.
	Unreachable — Shows that an active session, or attempt to connect a session has timed out. A service node can also signal that it is unreachable.

Rating	The relative capacity of the service to accept additional. sessions.
Identification	Shows a text string which identifies the service or describes how to use the service.

SHOW/MONITOR SERVICES SUMMARY Privilege: See Below

Use the SHOW/MONITOR SERVICES STATUS display to view a one-line summary about the availability of each service that is available on the network and/or locally available at the access server. .

Privileges

Secure and non-privileged users can use the SHOW SERVICES SUMMARY command, unless the DEFINE/SET PORT LIMITED VIEW is ENABLED. Only users at privileged ports can use the MONITOR SUMMARY STATUS command.

Syntax

```
SHOW/MONITOR SERVICE    [service-name]    SUMMARY
                        [LOCAL]
                        [ALL]
```

Where	Means
service-name	Specifies that the access server will display the requested information about one or more specific services that are available on the network to the user at the port where the request is made. You can specify a wildcard character to select a subset of the *service-names* to be displayed. The asterisk symbol (*) is the wildcard character. For example, if one types SHOW SERVICES AB*, the server will display all accessible *service-names* whose names start with AB. SHOW SERVICES A*BC displays accessible *service-names* whose names start with A and end with BC.
ALL	Specifies that the access server will display the requested information about all services that are available on the network to the user at the port where the request is made.
LOCAL	Specifies that the access server will display the requested information about all services that are available locally on the access server to the user at the port where the request is made.

Example

```
Xyplex>> show service summary

Service Name        Status       Identification

1C323               Available
1C325               Available
1C326               Available
277B2               Available
720HUB              Available    Miller's hub
CON_XANTH           Available
CORPMODEM           Available
ENGLASER            Available    HP LaserJet II (Lower Deck)
ENGLP               Available    hi-speed wide carriage (lower deck)
ENGSVC              Available
ENG_SYSPRINT        Available    Hi-speed narrow carriage (lower deck)
ESC_LASER           Available
MODEM                      Available
SSEALPHA            Available      SSE Dec 3000 Alpha / OpenVMS AXP
TEST                Available
```

MONITOR/SHOW SERVICES SUMMARY Display

The following table describes each of the items (fields) of data in the MONITOR/SHOW SERVICES SUMMARY display.

Field	Description
Service Name	The name of a service on the network.
Status	The whether or not the service is currently reachable or available. The possible values which can be shown include:
	Available — Shows that at least one service node that offers the service has the status REACHABLE.
	n Connected — Shows that the service is reachable, and that the server has n currently active sessions with this service.
	Unavailable — Shows that all service nodes that offer the service have the status UNREACHABLE.
	Unknown — Shows that none of the service nodes that offer the service have the status REACHABLE, and that at least one of these service nodes has the status UNKNOWN.
Identification	Shows a text string which identifies the service, or describes how to use the service.

SHOW/MONITOR SESSIONS Privilege: N, S, P

Use the SHOW/MONITOR SESSIONS command to display information about service sessions for server ports.

Privileges

Secure and non-privileged users can use the SHOW SESSIONS command SECURE users can only display information about the port they are logged on to.

Syntax

```
SHOW/MONITOR SESSIONS [PORT port-list]
                      [ALL]
```

Where	Means
PORT	Display service session information about one or more ports.
port-list	The port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.
ALL	Display service session information about all ports on the server.

Example

```
Xyplex>> show sessions
Port  0: system            Service Mode            Current Session NONE
```

MONITOR/SHOW SESSIONS Display

In the session display, the first line of information for each port shows port-related information. The line(s) which follow the port-related information list(s) active session information. When a session is terminated, the information for the session is removed and replaced by the information below it in the display. The following table describes the fields on the MONITOR/SHOW SESSIONS display:

Port Information

Field	Description
Port n	The number of the physical server port, about which the system is displaying information.
Service Mode	The current port mode (either Local Mode or Service Mode).
Current Session n	The number of the currently active session.

Session Information

Session n	The number of the session.	
Status	The current status of the session. The values that can be displayed are:	
	Available	The port, whose ACCESS characteristic is set to REMOTE or DYNAMIC, is not busy.
	Connected	The port is currently connected to a service.
	Disconnecting	A session is disconnecting from a service.
	Dealloc	The server is deallocating the resources from a session.
	Fail 2	A connection attempt has failed.
	FWait	The session is waiting for an internal resource in order to indicate to the software that a connection attempt has failed.

Quit	A session has been disconnected.
QWait	The session is waiting for an internal resource in order to indicate to the software that a session has been disconnected.
Retry	The session is retrying a connection.
Slot	The session is trying to find a LAT slot on the virtual circuit for this session.
Start	The server is allocating resources for this session.
Status	The session is sending the status of a connection (accepted or rejected) to the software.
SWait	The session is waiting for an internal resource in order to indicate the status of a connection (accepted or rejected) to the software.
Wait	The server is allocating resources for a remote session.

Service Mode	The service mode for the session. Valid service modes are:	
	Interactive	The server recognizes all special characters.
	Passall	The server passes all characters as data.
	Pasthru	The server recognizes the XON and XOFF characters, but passes all other characters on as data.
	Transparent	The server initially sets all sessions so that a Telnet session ignores Telnet option messages received from a remotely initiated session and does not send any Telnet option messages from the locally initiated session, in addition to disabling all switching characters, Telnet command characters, and XON/XOFF flow control recognition. For a LAT session, the server tells its partner it is PASSALL but acts locally as if it were PASTHRU.
	Controlled	Frames the session using the strings defined by the DEFINE/SET PORT CONTROLLED SESSION INITIALIZE/TERMINATE command. This controlled mode is independent of other service modes.
Destination (node)	The currently active LAT service or Telnet destination associated with a session. For LAT services, the display includes within parentheses the name of the service node. For a remote-access connection to the port, the service name is that of the LAT service sought by the requesting node and the name within parentheses is that of the requesting node. Note that if the destination is a domain-name which is too long to fit on the display, the name displayed is truncated and indicated by asterisk (*).	
Telnet options	If there is a second line of session information, it The Telnet options that have been negotiated for the session. The Telnet Echo and Binary options may be shown. The verbs "Do" and "Don't" indicate whether or not the server will perform that option. The verbs "Will" and "Won't" indicate whether or not the connection partner will perform the option	

SHOW UNIT Privilege: S, P

Use the SHOW UNIT command to display the hardware type, version, ROM version and software version, level, and protocol(s) available on the unit.

Syntax

```
SHOW UNIT
```

Example

```
Hardware Type:       86
Hardware Revision:   00.00.00
Rom Revision:        470000
Software Type:       Access Server Level 4
Software Revision:   V6.0.4S11
Protocol Type:       LAT, TELNET, RLOGIN, TN3270, ARAP, SNMP, PPP, IPX,
XPRINTER

Daemon(s):           LPD


Enabled Feature(s):  APD, HELP, INTERNET SECURITY, IP FILTERING,
IPX FILTERING, ULI, SECURID, MENU, NESTED MENUS,
KERBEROS, RADIUS

APD Message:
AutoProtocolDetect - Begin protocol or enter 4 returns for interactive mode.

MX1620>>                          Sample SHOW UNIT Display
```

The following table describes each of the columns in the SHOW UNIT display:

Field	Description
Hardware Type	The Xyplex-assigned hardware type for the unit. Refer to the *Software Kit Information* supplied with your software kit for a current list of available *device-types*.
Hardware Revision *xx.yy.zz*	The version of the access server hardware, where *xx* indicates the version of the access server cards, *yy* indicates the type of the MAXserver or Network 9000 chassis, and *zz* indicates the version of the MAXserver or Network 9000 chassis.
ROM Revision *xxxxxx*	The version, *xxxxxx*, of access server ROM software.

Software Type: Access Server Level *n*

Indicates the type of features that are available on this Xyplex unit. The value for *n* has the following meaning: , , and software version, level, and protocol(

1 MX-TSERV-J8 without V5.0 or subsequent enhancements.

2 MX-TSERV-J8 with only Internet Security and Telnet Console enhancements, but no other enhancements.

3 All other software products running 1 Megabyte load image.

4 Products running Multi-Megabyte load images.

Refer to the *Software Kit Information* supplied with your software kit for a current list of features that are supported on various types of Xyplex products.

Software Revision *x.yz*

The version of Xyplex TCP/IP-LAT software, where *x* indicates the major revision level, *y* indicates the minor revision level, and *z* is a letter/number combination indicating that the software is an Alpha (A), Beta (B), or Special (S) software release.

Protocol Type

Indicates which protocols (for example, LAT, TELNET, SNMP, RLOGIN, TN3270, ARAP, PPP, IPX, or Kerberos protocols) are enabled for this unit. Refer to the *Software Kit Information* supplied with your software kit for a current list of protocols that are supported on various types of Xyplex products.

Enabled Feature(s)

Indicates which features (for example, Help, Internet Security, Kerberos , MENU, or MULTISESSIONS features) are enabled for this unit. Refer to the *Software Kit Information* supplied with your software kit for a current list of features that are supported on various types of Xyplex products.

APD Message

When APD is enabled on the unit, the default message string is: "AutoProtocol Detect - Begin protocol or enter 4 returns for interactive mode."

The valid values are any message string of up to 80 characters. Make sure to enclose the message in quotes (").

SHOW/MONITOR USER STATUS Privilege: N, P

Use this command to display the current status for all serial ports. From this display you can also view a grand total of this information for all ports combined. For optimum display, use a 132-column terminal display.

Syntax

SHOW USER STATUS

```
Xyplex>> show user status
                                          08 Oct 1998  09:14:35

P#  Control Lines       Speed     Char Tx   Char Rx   Parity Errors Overrun Errors Framing Errors
--  -------------       -----     -------   -------  -------------  -------------- --------------
 1  DTR, RTS  DSR, CTS   9600      204187     66            0              0              1
 2  DTR, RTS  DSR       38400          0       0            0              0              0
 3  DTR, RTS  DSR       38400          0       0            0              0              0
 4  DTR, RTS  DSR       38400          0       0            0              0              0
 5  DTR, RTS  None      38400          0       0            0              0              0
 6  DTR, RTS  None      38400          0       0            0              0              0
 7  DTR, RTS  None      38400          0       0            0              0              0
 8  DTR, RTS  None      38400          0       0            0              0              0
-------        -------              -------------            --------------         --------------
Totals:                              204187     66            0              0              0
```

Where	Means
Port #	The port number.
Control lines	Current modem/control lines.
Speed	Current line speed of each port.
Char Tx	Displays the total characters transmitted since the last clear was issued.
Char Rx	Displays the total characters received since the last clear was issued.
Parity errors	Displays the number of parity errors since last clear was issued.
Overrun Errors	Displays the number of overrun errors since last clear was issued.
Framing Errors	Displays the number of framing errors since last clear was issued
Totals	Grand totals for all ports

SHOW/MONITOR USERS — Privilege: N, P

Use this command to determine which ports are logged on, and the name of the user who is logged on to the port.

Syntax

```
SHOW/MONITOR USERS
```

Example

```
Xyplex>> show users
                                          08 Oct 1998  09:14:51
Port    Username             Status          Service

  0     system               Executing Cmd
  1     J.P. Jones           Wait Input
  8           (Remote)             Connecting      (Remote Connect)
```

MONITOR/SHOW USERS Display

The following table describes each column on the MONITOR/SHOW USERS display:

Field	Description
Port	The port number about which the system is displaying information.
Username	This column lists the name given by the user to log on to the port, the name given to the port using the PORT USERNAME, or "(Remote)" for ports which have a remote connection (i.e., a host-initiated connection).
Status	The current status of the port. The possible values are:
	Autobaud — The port is being autobauded.
	Available — A port set to REMOTE or DYNAMIC is not busy.
	Check Modem — The port is verifying that modem signals are properly asserted.
	Check Connect — The port is determining the status (accepted or rejected) of a pending connection.
	Connected — The port is currently connected to a LAT service or Telnet destination.

Connect Wait	The port is waiting to retry a connection attempt (used when PORT AUTOCONNECT is set to ENABLED). are logged
Connecting	The port is currently attempting to connect to a LAT service or Telnet destination.
Dialback Wait	The Port is waiting for the remote modem to answer a dial-back call.
Disconnected	Shows that a session was disconnected (for example, for being inactive for too long).
Disconnecting	Shows that a session is disconnecting from a LAT service or Telnet destination.
Executing Cmd	The port is executing a command from the access server local command mode.
Finding Script	The port is searching for a script file via TFTP read requests.
First Dialback Login	The port is making its first attempt to locate a dial-back script.
Idle	Shows that the port is not in use.
Loading Script	The port has located a script file and is receiving the file from the script server.
Local Mode	The port is logged on to the server, and is in the local command mode.
Locked	Shows that the user has used the LOCK command to disable the port.
Login	The port is waiting for the user to enter a login or Kerberos password.

Login Wait	The port has been disabled (for 60 seconds) because an incorrect password has been entered, or because a dial-back attempt has failed. are logged
Password	The port is waiting to enter the password required by a password-protected LAT service.
Reset	The port is reverting to its stored configuration.
Retry Connect	The port is trying to connect to a service that was previously unavailable (used when PORT AUTOCONNECT is set to ENABLED).
Running Script	Shows that the port is executing the commands contained in a script file.
Second Dialback Login	The port is making its second attempt to locate a dial-back script (the port searches the directory path "above" the path specified for this script server).
Slip	The port is a SLIP port.
Suspended	The user has entered the local-switch character, and the session is being suspended.
Test Wait	The port is performing a TEST SERVICE command.
Test Out	The port is outputting the results of a TEST SERVICE command.
Wait Input	The port is at the local prompt (waiting for the user to enter a command).
Wait Logout	The port is waiting for modem control signals to be deasserted.
Wait Output	The port is completing display output before logging out.
Wait Queue	A connection request from this port is in a queue.

Wait Session	The session is being disconnected.
Service	The currently active LAT service or Telnet destination, or the service connection that was interrupted when the user entered local mode. If a remote connection has been formed with the port, the service will be displayed as (Remote Connect are logged

SHOW XPRINTER Privilege: N, P

The SHOW/LIST XPRINTER command shows you the names of all Novell printer servers that are assigned to local Xyplex access server or printer server ports.

You use the Novell PCONSOLE utility to create Novell printer servers. (Do not confuse the term Novell printer server with a Xyplex printer server, such as a MAXserver 1450 or 1400A Printer Server unit.) Novell printer servers can be assigned to a serial or parallel port on a Xyplex access server or printer server. You can view the name of any Novell printer server that is assigned to a port on a Xyplex access server or printer server using this command.

See the *Printer Configuration Guide* for a discussion of Novell printing in the XPRINTER environment.

Syntax

```
SHOW XPRINTER
```

Example

```
Xyplex>> show xprinter

 Available Print Servers
ENGINEERING_PRINTER_SERVER
MANUFACTURING_PRINTER_SERVER
```

SHOW XPRINTER Display

SHOW/LIST XPRINTER PORTS Privilege: N, P

The SHOW/LIST XPRINTER PORTS command shows you the status of ports which have local XPRINTER services.

Novell printer servers can be mapped to a physical port on an access server or printer server. The port can be either a serial port or a parallel port. Each Xyplex access server or printer server port can be connected to only one Novell printer server. You can view the status of XPRINTER activity using the SHOW/LIST XPRINTER PORTS command.

See the *Printer Configuration Guide* for a discussion of Novell printing in the XPRINTER environment.

Syntax

```
SHOW/LIST XPRINTER PORTS [port-list]
                                [ALL]
```

Where	Means
port-list	Represents the Xyplex access server or printer server ports which have local XPRINTER services assigned to them. If you want to view the status of more than one port, you can specify the individual port numbers separated by commas or specify a range of port numbers separated by a hyphen, or a combination of both (do not include spaces). For example, the *port-list*: 1,3-4 refers to the individual port settings: 1, 3, and 4.
ALL	The status of all Xyplex access server or printer server ports which have local XPRINTER services assigned to them.

Example

```
Xyplex>> show xprinter ports 1-8

Port  State         Print Server    Printer #     Status
  1    Idle
  2    Idle
  3    Idle           PRINTER              3
  4    Idle
  5    Idle
  6    Idle
  7    Idle
  8    Idle
```

SHOW/LIST XPRINTER PORTS Display

TELNET CONNECT — Privilege: S, P

Use this command to establish a session by creating a virtual connection between your port (terminal) and a Telnet destination. When you use the TELNET CONNECT command, without specifying a domain name/ internet-address and telnet-port number, the access server will attempt to establish a session with a Telnet preferred destination, when one has been defined.

Syntax

```
TELNET [CONNECT]  [domain-name[:telnet-port number]]  [CONTROLLED]
                  [internet-address[:telnet-port number]]
```

Where	Means
CONNECT	An optional keyword.
domain-name	The logical name of the Telnet destination that will be the connection partner in a session with the port which you are logged on to. If the specified domain-name is not a fully qualified domain-name, the specified name will be concatenated with the default domain-name-suffix. The first time the server attempts to connect to any *domain-name* (following initialization) takes 2 seconds to occur because the server must locate a Domain Name Server and then attempt the connection. Subsequent attempts to connect to a *domain-name* occur with no delay, because the server already knows the location of a Name Server.
internet-address	The identity or location on the network of the Telnet destination that will be the connection partner in a session with the port which you are logged on to.
:telnet-port number	The number of the target Internet protocol or physical port number that is used in the session between the port you are logged on to and the connection partner (e.g., host or access server). The colon character (:) is required as syntax to separate the telnet-port number from the domain-name or internet-address. The default value is specified by the PORT TELNET DEFAULT PORT characteristic.
CONTROLLED	Frames a session with strings specified by the DEFINE/SET PORT CONTROLLED SESSION INITIALIZE/TERMINATE command.

TELNET CONNECT (continued)

Examples

1. `Xyplex> TELNET CONNECT FINANCESUN.XYPLEX.COM` to establish a session

   Establish a session between this port and the Telnet destination whose *domain-name* is FINANCESUN.XYPLEX.COM. Note that the user did not specify a *telnet-port number*. The access server will use the default *telnet-port number* (defined by the PORT TELNET DEFAULT PORT characteristic).

2. `Xyplex> TELNET 128.10.2.30:23`

   Establish a session between this port and the Telnet destination whose *internet-address* is 128.10.2.30. Note that the user specified a *telnet-port number* (23 in this case).

3. `Xyplex> TELNET CONNECT`

   Establish a session between this port and the preferred Telnet destination that the user or access server manager has defined for the port.

4. `Xyplex> TELNET CONNECT FINANCESUN.XYPLEX.COM CONTROLLED`

   This is the same as Example 1, except that the CONTROLLED option sends a string of hexadecimal characters to the console out of the asynchronous port when the connection is established. This string is defined using the DEFINE/SET PORT CONTROLLED SESSION command. For example, the string could set VT100 mode on the terminal. When logging or switching out of this session, a different hexadcimal string is sent (such as a string to exit VT100 mode).

1. Use this command to establish a session by creating a virtual connection between a access server port (this is called the "target" port), and a Telnet destination. The target port is usually a port other than the port you are currently logged on to. to establish a session

To use this command, you must specify the name of a Telnet destination. This can be done either by the TELNET CONNECT PORT command, or by defining a dedicated or preferred service for the target port. The target port can not have a session in progress (you can terminate the session using the LOGOUT PORT or DISCONNECT PORT command).

Syntax

```
TELNET [CONNECT] [PORT port number] [domain-name[:telnet-port number]]
                                    [internet-address[:telnet-port number]]
```

Where	Means
CONNECT	An optional keyword.
PORT	Specifies that you will connect a target port to a Telnet *domain-name/internet-address* and *telnet-port number*.
port number	Specifies the number of the target access server port which will be connected to a Telnet *domain-name/internet-address* and *telnet-port number*.
domain-name	Specifies the logical name of the host or server that will be the connection partner in a session with the target port. If the specified *domain-name* is not a fully qualified *domain-name*, the specified name will be concatenated with the default Internet *domain-name-suffix*. Note that the first time the server attempts to connect to any *domain-name* (following initialization) takes 2 seconds to occur because the server must locate a Domain Name Server and then attempt the connection. Subsequent attempts to connect to a *domain-name* occur with no delay, because the server already knows the location of a Name Server.
internet-address	Specifies the identity or location on the network of the host or access server that will be the connection partner in a session with the target port.

TELNET CONNECT PORT (continued)

:telnet-port-number	Specifies the number of the target Internet protocol or physical port number that is used in the session between the target port and the connection partner (i.e., the Telnet destination). Note that the colon character (:) is required to separate the *telnet-port number* from the *domain-name* or *internet-address*. to establish a session

Examples

1. `Xyplex>> TELNET CONNECT PORT 5 LASER`

Meaning: Establish a session between the target port (port 5) and the host or access server whose domain-name is LASER.

2. `Xyplex>> TELNET PORT 5`

Meaning: Establish a session between the target port (port 5) and the dedicated or preferred service, and default telnet-port number (defined by the PORT TELNET DEFAULT PORT characteristic) that the user has defined for the port.

3. `Xyplex>> TELNET CONNECT PORT 5 FINANCEVAX.XYPLEX.COM`

Meaning: Establish a session between the target port (port 5) and the host or access server whose domain-name is FINANCEVAX.XYPLEX.COM. Note that the user did not specify a telnet-port number. The access server will use the default telnet-port number (defined by the PORT TELNET DEFAULT PORT characteristic).

4. `Xyplex>> TELNET CONNECT PORT 5 128.10.2.30:23`

Meaning: Establish a session between the target port (port 5) and the host or access server whose internet-address is 128.10.2.30. Note that the user specified a telnet-port number (23).

TELNET CONSOLE — Privilege: N, P

This command enables a user to access the remote console port of a access server (port 0) via Telnet. While connected to port 0, the user interface is identical to the interface when the REMOTE CONSOLE command is used. The target console portcannot have a session in progress. Once you are connected to the remote console port of a access server, you can connect to another access server's remote console port via Telnet. (You cannot access another remote console port this way using the REMOTE CONSOLE command.)

Additionally, you can suspend a Telnet session with the remote console port of one access server (e.g., by pressing the BREAK key) and then initiate a session with another access server's remote console port. You can then suspend that Telnet session and resume the original session, or initiate a session with the remote console port of a different access server.

The Console LED will remain lit whenever there is either a local or remote console session.

The following port settings are predefined for the remote console port of a access server. You cannot change these settings.

Characteristic	Setting
ACCESS	LOCAL
AUTOBAUD	DISABLED
BREAK	DISABLED
CHARACTER SIZE	8
DEDICATED SERVICE	NONE
DIALUP	DISABLED
DSRLOGOUT	DISABLED
DTRWAIT	DISABLED
FLOW CONTROL	XON
INPUT FLOW CONTROL	ENABLED
INPUT SPEED	9600
MODEM CONTROL	DISABLED
OUTPUT FLOW CONTROL	ENABLED
OUTPUT SPEED	9600
PARITY	NONE
SPEED	9600

Syntax

```
TELNET CONSOLE    [internet-address[:telnet-port number]]
                  [domain-name[:telnet-port number]]
```

TELNET CONSOLE (continued)

Where	Means
internet-address	The identity or location on the network of the Telnet destination to which you want to establish a session.
domain-name	The logical name of the destination to which you want to establish a Telnet session.
:telnet-port number	The physical port number to which you want to establish a Telnet session. The default is 2000. settings

Examples

1. `Xyplex>>TELNET CONSOLE 117.29.10.30`

Meaning: Establish a Telnet session with the remote console port (in this case port 0) of the access server whose Internet address is 117.29.10.30

2. `Xyplex>>TELNET CONSOLE FINANCEVAX.XYPLEX.COM`

Meaning: Establish a Telnet session with the remote console port of the access server whose domain name is FINANCEVAX.XYPLEX.COM. The access server uses the default Telnet port number, 2000.

TEST IP — Privilege: N, P

Use this command to display how the server communicates with a specified Telnet destination (i.e., perform an Internet "ping".

The server will display one or more internet-addresses which represent the round-trip path that it would use to communicate with the specified Telnet destination

Syntax

```
TEST IP        [domain-name]        [RECORDROUTE]
                                    [NORECORDROUTE]*
               [internet-address]   [RECORDROUTE]
                                    [NORECORDROUTE]*
```

Where	Means
RECORDROUTE	Specifies that the server will ask that the route, by which it communicates with the specified destination, be recorded in the packet. The server will display one or more *internet-addresses* which represent the round-trip path that it would use to communicate with the specified Telnet destination.
NORECORDROUTE	Specifies that the the server will not ask that the route, by which it communicates with the specified destination, be recorded in the packet. The server will display only the source and destination *internet-addresses*. This is the default for the TEST IP command.

TEST LOOP Privilege: P

When you use the TEST LOOP command, the server tests the physical connection between itself and a LAT service node. The server will display a message indicating whether or not the test was successful. As a TEST LOOP command option, you can specify that an assistant node relay transmission for both outgoing and/or incoming transmissions. For example, you can specify an assistant node at the far end of the Ethernet network so that the test pattern is transmitted along the full length of the network.

Syntax

```
TEST LOOP ethernet-address-t][Count n] [Width n][Help Full Assistant]  [ethernet-address-h]
                                                [Help Receive Assistant] [ethernet-address-h]
                                                [Help Transmit Assistant] [ethernet-address-h]
```

Where	Means
Count n	The number of times the test will be repeated. Valid values for n are whole numbers in the range of 1 to 65535. The default value is 1. If you specify NONE, the tests run continuously until you press the BREAK key or type the local switch character.
Width n	The number of data characters per packet. Valid values are whole numbers in the range of 1 to 1470. The default is 0.
Help Full Assistant	Specifies that you wish to have an assistant node relay transmission for both outgoing and incoming transmissions.
Help Receive Assistant	Specifies that you wish to have an assistant node relay transmissions coming into the access server.
Help Transmit Assistant	Specifies that you wish to have an assistant node relay transmissions coming from the access server.
ethernet-address-h	The unique Ethernet address of the assistant node. Valid values are in the form of six pairs of hexadecimal numbers which are separated by hyphens (e.g., AA-01-04-C9-56-F1). This address must be different than the address of the access server or the target service node. Multicast addresses are not permitted.

TEST PORT — Privilege: See Below

When you use the TEST PORT command, the server tests the physical connection between itself and a device attached to the port. To end the test at any time, press the BREAK key (if enabled) or the local switch character. The server will display a repeating pattern of characters that you can observe and check for errors.

Privileges

Non-privileged users can use TEST PORT to verify correct operation of their own port. Only users at a privileged port can use the TEST LOOP command, or use the TEST PORT command to verify operation of a port other than their own port.

Syntax

```
TEST PORT port number [COUNT n] [WIDTH n] [LOOPBACK]  [EXTERNAL]
                                                      [INTERNAL]
```

Where	Means
COUNT n	The number of times the test will be repeated. Valid values for n are whole numbers in the range of 1 to 65535. For port tests, the default value is 23. If you specify NONE, the tests run continuously until you press the BREAK key or type the local switch character.
WIDTH n	The number of characters per line. Valid values for are whole numbers in the range of 1 to 132. The default value is 80. Notes: If you are using the Count and Width keywords together, Count must precede Width in the command. If your port speed is 38400, the output will appear to be slow unless you set the Width to a value greater than 25.
LOOPBACK	The loopback test will be performed on the local or remote port to be tested (this is always a port other than the port where the test is initiated).
EXTERNAL	The loopback test will be performed by placing a loopback connector on the port to be tested (i.e., in a loopback connector, the transmit data and receive data pins are tied together).
INTERNAL	The loopback test will be performed by an internal programmable hardware connector on the port to be tested.

TEST SERVICE Privilege: P

When you use the TEST SERVICE command, the server tests the end-to-end communication between the port and a LAT service node. The server will send a pattern of characters to the specified service. To end the test at any time, press the BREAK key. The server will display a message indicating whether or not the test was successful.

Syntax

TEST SERVICE *target-information test-options*

The syntax for the *target-information* is:

[*service-name*][NODE *node name*][DESTINATION *port name*]

The syntax for the *test-options* is:

[COUNT *n*][WIDTH *n*][LOOPBACK] [EXTERNAL]
[INTERNAL]

Where	Means
service-name	The name of the service to be tested.
NODE	A specific node will be used to perform the test, when the service specified by service-name is offered at more than 1 node.
node name	The name of the node to be used for a test.
DESTINATION	Specifies that you will perform the test to a specific remote port.
COUNT n	The number of times the test will be repeated. Valid values for n from 1 to 65535. The default value is 1. If you specify NONE, the tests run continuously until you press the BREAK key or type the local switch character.

WIDTH n	The number of characters per line for port or service tests, or the number of data characters per packet for loop tests. For port or service tests, valid values for are whole numbers in the range of 1 to 132. For port or service tests, the default value is 80. For loop tests, valid values are whole numbers in the range of 1 to 1470. For loop tests, the default is 0. .
LOOPBACK	Define how a loopback test will be performed on the local or remote port to be tested (this is always a port other than the port where the test is initiated).
EXTERNAL	The loopback test will be performed by placing a loopback connector on the port to be tested (i.e., in a loopback connector, the transmit data and receive data pins are tied together.
INTERNAL	The loopback test will be performed by an internal programmable hardware connector on the port to be tested.

ULI — Privilege: N, P

Use the ULI command to execute UNIX-like commands, for users who are using the DECserver-like command interface. To use this command, the ULI must be enabled at the server and port, but not activated.

The UNIX-like interface is only available on certain multi-megabyte load images. Refer to the kit information supplied with your software kit for more information. Also refer to the *Using the ULI Guide* for more information about ULI.

Syntax

`ULI [uli-command]`

Where	Means
uli-command	The ULI command that you want to perform. You can activate the ULI by typing ULI by itself (i.e., without including a *uli-command*).

Examples

```
1. Xyplex> ULI
   Xyplex%

2. Xyplex> ULI netstat
```

XCONNECT Privilege: S, P

Use the XCONNECT command to establish a session with an XDM host. You can either provide the domain name or Internet address of an XDM host in the command line, or simply enter the XCONNECT command. If you enter the command without specifying a host, the access server searches the permanent database for a host that was specified with the DEFINE PORT XDM host command, or uses the BROADCAST query type.

Syntax

XCONNECT [*domain-name /internet-address*]

Where	Means
domain-name	The domain name of the XDM host.
internet-address	The Internet address of the XDM host.

Examples

1. Example 1 assumes that that you have already defined an XDM host, or the BROADCAST query type. When the user enters the command, the UNIT either searches for the specific or indirect host, or broadcasts a query to the network.

```
Xyplex> xconnect
```

```
Welcome to the Xwindow System

Login:

Password:
```

2. Example 2 assumes that you have not defined an XDM host, so the user enters the Internet address of the host with the XCONNECT command.

```
Xyplex> xconnect 143.129.80.200
```

```
Welcome to the Xwindow System

Login:

Password:
```

ZERO COUNTERS — Privilege: S, N, P

Use this command to reset counters displayed by the SHOW/LIST/MONITOR SERVER, NODES, and/or PORTS commands.

Privileges

Secure and non-privileged users can use the ZERO COUNTERS PORTS command to reset the counters for their own port. All other ZERO COUNTERS commands are privileged only.

Syntax

```
ZERO [COUNTERS]   [NODE node name]
                  [PORT port-list]
                  [ALL]
```

Where	Means
NODE	The server will reset the counters that relate to a specific node. This is the default.
node name	The name of the node about which the server counters will be reset.
PORT	The server will reset the counters that relate to a specific port.
port-list	The port number(s) of the ports for which the counters will be reset.
ALL	The server will reset all counters for all displays.

Example

1. `Xyplex>> ZERO COUNTERS NODE FINANCEVAX`

Meaning: Reset to zero the counters that relate to the service node named FINANCEVAX

2. `Xyplex>> ZERO PORT 1-3`

Meaning: Reset to zero the counters that relate to ports 1 through 3 on the access server.

3. `Xyplex>> ZERO ALL`

Meaning: Reset to zero all counters in the displays shown by the SHOW/LIST/MONITOR SERVER, NODES, and/or PORTS commands.

Index

abort output character, 247
access types, 82, 623, 667
account logging
  Radius, 487
accounting
  accepting registration requests, 495
  maximum number of entries, 317
  RADIUS, 228
  remote logging, 337
  syslogd output, 337
  verbose mode, 531
accounting logs, 216, 688, 689
  current values, 656
accounting logs, 686, 687
ACE/Servers. See SecurID., 509
ACK bit, 371
ACK enabled, 431
ACK packets
  ACK delays, 513
acknowledge bit setting, 371
ACM_PORT, 506
ACMBASETIMEOUT, 504
ACMMAXRETRIES, 505
alternate port characteristics, 628 - 630
alternate keymapping
  TN3270 devices, 521
announcements, 318
ANSI
  escape sequences, 297
  screen colors, 523
  terminal displays, 598
APD
  authentication, 85
  default port settings, 86
  enabling, 319
  message strings, 320
  port settings, 84
  prompt settings, 87
  timeout, 88
AppleTalk
  default zones, 321
  node names, 323
  zone access, 94
AppleTalk Remote Access Protocol. See ARAP.
  89, 473
ARAP
  connection time, 93
  current settings, 632
  default zones, 321
  displaying counters, 634, 635
  displaying current settings, 633
  enabling, 473
  guest logins, 91
  maximum connection time, 92
  node names, 323
  port settings, 89
  server settings display, 693
  zone access, 94
areas
  flash cards, 546
ARP table, 47
ASCII control characters
  PPP sessions, 195
ASCII file transfers, 597
ASCIITOEBCDIC translations, 755, 756
attention character
  Telnet, 248
authentication
  APD, 85
  CHAP password, 471
  displaying banners before, 304
  Kerberos version 5, 422
  PPP PAP, 218
  Radius, 486
  Radius servers, 492
  SecurID, 503, 505
  SNMP traps, 382
authorized groups, 95, 130
auto-answer mode, 331
autobaud, 641, 667
  port settings, 96
autoconfigure, 389
autoconnect, 97, 641
autodedicated, 98, 641
autodiscovery, 354, 355
autohangup, 99, 641
Automatic Protocol Detection. *See* APD.
autoprompt, 100, 641
autosend, 142
background sessions, 174
backspace character, 172
backward switch, 25, 101
backwards command, 25
baud rates, 245
  port settings, 83, 96
begin line character, 172
bell character, 176, 184
binary file transfers, 596
binary session mode, 249
bit values, 246

bits per character, 108
blinking screen, 292
BREAK key
  defining action, 102
break keys, 146
break sequences
  Telnet, 295
breaks
  defining length of break time, 103
  Telnet types, 269
broadcasts, 641
  IP addresses, 356
  IPX RIP information, 158
  IPX RIP timeout settings, 406
  IPX RIP timer settings, 407
  IPX SAP settings, 210
  IPX SAP timer settings, 413
  message display settings, 104
  RIP information, 405
  SAP information, 411
  sending messages, 26, 27
  server settings, 324
buffer size
  command input, 110
  Tn3270 sessions, 291
buffered transmissions
  Telnet, 293
buffers, 463
  typeahead setting, 298
bypassing offline printers, 450
bypassing UNIX host logons, 500
cabling types, 179
cancel character, 172
carriage-return characters, 271
CCL scripts
  current settings, 694
  defining the location, 107
  deleting, 44
  modem speaker settings, 105
  reloading, 572
  server names, 106
CHAP
  challenge size, 488
  challenge timer settings, 193
  RADIUS authentication, 194
character maps, 195
character settings
  line editing characters, 607
character size
  current port settings, 637
  defining, 108
check timer period, 28
circuit timer settings, 329
CLEAR commands, 29, 31
clear screen function, 297
clear services command, 57
colors
  screen settings, 292
  TN3270 screens, 523
command input buffer size, 110
command lines
  editing, 171
  maximum length, 20, 70, 309
communications
  checking LAT services, 789, 790
compressed SLIP (CSLIP), 136
compression, 136, 207
  current settings, 660
connect command, 60
connect port command, 63
connecting LAT sessions, 551
connecting to TCP/IP destinations, 135
connection queue requests, 541
connection queues, 226, 485
  deleting, 577
  LAT service display, 683, 684
  LAT services, 684
connection requests
  job numbers, 683
connection strings
  defining for sessions, 113
connection types
  defining, 84
  local or remote access, 687
connections, 132
  ARAP session time, 93
  checking, 787
  creating an IP rotary, 376
  creating for Telnet, 780, 781, 782, 783
  current status, 615
  default port protocols, 86
  establishing host or service sessions, 60, 61
  group access, 511
  inbound restrictions, 109
  Kerberos, 426
  ports, 63
  queue limits, 485
  restricting, 243
  resuming, 111
  security, 138
  service settings, 539
  TCP/IP, 135
  time limits for ARAP, 92
  useradata delays, 530
connectresume, 111. 641
console LED, 28, 574, 784
console ports, 574, 784
controlled ports, 112, 331, 645
controlled session command, 113
copying files, 589

copying flash cards, 325
copying port settings, 129
counters
ARAP, 634, 635
IP ICMP server display, 710, 711, 712
IP server settings, 706, 707, 708
LPD, 733, 734
port acitivity, 646
PPP IP, 661
PPP ports, 657, 658
resetting to zero, 793
server counters displays, 699 - 702
SNMP, 720 - 722
TCP server settings, 708
UDP server settings, 709
CRASH command, 66
crash dump procedure, 66, 340
CSI escape sequences, 254
CSLIP, 136
CTRL characters, 101
cursor control functions, 297
daemons
fingerd, 333
LPD, 334
routed, 335
rwhod, 336
syslogd, 337
data leads only mode, 179
data transparency, 596
databases
maximum IP routes, 377
permanent or temporary changes, 327
routing table entries, 377
date settings
server, 339
DCD timeout settings, 114
DCD/DTS flow control, 186
DEC terminal support, 180
DECnet NCP TRIGGER command, 451
dedicated service, 98
defining, 115, 116
description, 233
LAT ports, 168
Telnet, 255
default zones
ARAP, 321
defaults
initialization records, 442
line editing characters, 608
logon messages, 534
port parameters, 529
port settings, 296, 641
server parameters, 529
Telnet characters, 678
Telnet port numbers, 282
Telnet ports, 784, 785
TN3270 session port numbers, 281
TN3270 translation table, 569
UDP port for Radius accounting, 487
DEFINE and SET commands
descriptions of, 67
defragmentation of packets, 361
delay values, 530
delays, 696
delete begin character, 172
delete line character, 172
deleting
domain names, 558
flash cards, 344
IP routes, 46
IP security entries, 562
IPX RIP export filters, 37
IPX SAP filters, 39
LAT services, 570
parameter servers, 35, 563
queue entries, 577
RIP import filters, 38
rotary entries, 45
script servers, 567
security table entries, 36
server menu entries, 566
TN3270 translation tables, 569
delimiters
DTFTP loading, 434
file settings, 364
destination filters, 367
destinations
displaying, 604
device names
adding to TN3270 keymaps, 525
printer ports, 287
device tables
copying, 517
creating, 517
server settings, 517
device types
displaying, 609
global, 559
TN3270, 517 - 525
dial out port settings
dial up, 642
dial up lines
defining, 122
dialback, 642, 667
port settings, 119
script commands, 119
timeout settings, 120
timeout settings, 630
discard characters, 123
disconnect

remote console sessions, 330
send warnings, 230
session codes, 688
disconnect commands, 543
disconnected sessions, 674
displays
IBM3270 stations, 167
restrictions, 170
server screen types, 695
welcome messages, 534
DNS servers
defining, 68
domain name servers, 68
IP addresses, 359
IP addresses, 359
domain name suffixes
default settings, 357
default settings, 357
description of, 22
domain names
defining, 68, 69, 363
deleting, 32, 558
description of, 22
displaying, 604, 605
Kerberos, 427
learned, 32, 68
locally defined, 32
naming conventions, 22
RLOGIN, 581
rotary groups, 68
rules for, 68
SecurID servers, 509
servers, 374
time to live settings, 365
XDM hosts, 305
Xremote font servers, 537
DSRLOGOUT, 124, 243, 642
DSRWAIT, 125, 642
DTFTP image loading, 433, 437
DTR signals, 126
DTRWAIT, 126, 630
Dual Session Management
DEC terminals, 180
enabling terminals, 456
dump file, 66, 340
dump server protocols, 341
dump storage servers
displaying status, 609
dynamic access ports, 82
EBCDICTOASCII translations, 755, 756
echo commands display, 237
echo modes (Telnet), 264
EIA interface signals, 179
encryption mode
SecurID, 507
end of line character, 172
end of record (EOR), 265, 284
erase line character, 267
erasing flash cards, 326
error checking, 187
error codes
accounting logs, 689
disconnects, 688
error locks, 285
error messages
CCL scripts, 573
console commands, 496
defining for Kerberos, 421
display settings, 178
heartbeat commands, 496
Kerberos 4, 727, 728
Kerberos 5, 729
modems, 496
server displays, 496
errors
discarding characters, 123
framing errors, 647
notify users when lost data occurs, 176
server memory dumps, 340
SNMP, 722
escape sequences
ANSI-standard, 523
Telnet, 254
Ethernet addresses
image file location, 546
parameter servers, 542
Ethernet-type packets, 404
EtherTalk zones, 321
event logging, 343
exiting from a MONITOR display, 598
exporting, 37, 161, 414
failure limits, 200
fatal errors
server memory dumps, 340
faults, 691
field settings
insert mode, 289
FIFO order, 683
file delimiters
defining, 364
during DTFTP loading, 434
file transfers
binary mode, 249
in ASCII, 249
filenames
images, 435
load files, 362
script naming conventions, 583
server software, 498
filtering

displaying current settings, 630
Telnet newline sequences, 272
usernames, 301
filters
defining destinations, 153
deleting IPX SAP import, 41
destination ports, 150
IP traffic, 147, 148
IPX RIP import, 38
IPX SAP, 39
TCP SYN, 151
Finger User Information Protocol. See fingerd, 333
fingerd
enabling, 333
flash cards. See also memory.
areas, 546
copying contents to another card, 325
copying files, 589
deleting contents, 326
displaying current settings, 601, 602
displaying information, 609
formatting, 344
loading images, 345
retrieving load images, 546
terminating updates, 547
flow control, 249
CTS/RTS settings, 127
defining, 127
input data communications, 134
port settings, 186
RTS/CTS settings, 127
Telnet RS491, 278
font servers
XDM host, 537
Xremote, 537
formatting flash cards, 344
formfeed settings, 447
forwards character, 172
forwards command, 544
forwards switch character, 544
fragmentation
reassemble packets, 361
framing errors, 647
gateway routers, 436
gateways
IP addresses, 372
routing table entries, 379
global devices, 559
group codes, 95
group lists
defining, 95
groups
allowing connections to services, 511
defining port authorization, 95
displaying at ports, 130
providing server access, 510
removing from the database, 483
guest logins
ARAP, 91
guest users
login as, 91
handshaking, 127
EOR messages, 265
hang up ports automatically, 99
hanging printer, 628
hardcopy devices, 598
hardcopy terminals, 297
hardware addresses
displaying, 609
hardware faults, 691
hardware flow control, 186
hardware types
display current settings, 559, 771, 772. See also *Software Kit Information*.
HDLC settings
displaying, 658
heartbeat commands error messages, 496
heartbeat signals, 346
Help command, 548
Help settings, 347
IBM 3270 display station functions, 167
ICMP
re-direct messages, 335, 499
routing messages, 378
identification messages, 348
length of, 349
identifying network trouble or server problems., 691
idle ports, 668
idle time limits, 293
idle timeouts, 133, 648
current settings, 628
IEE 802.2
(RAW) type packets, 404
IEEE 802.3
(MAC) type packets, 404
image files
loading, 345
loading protocols used, 350
image loading
DTFTP, 434
filenames, 435
path names, 435
terminating, 547
immediate transmission (Telnet), 293
importing filters
description, 38
importing route tables, 157
inactive ports, 351, 391

inactivity timer, 642
increment-value
local server TCP ports, 375
INIT DELAY command, 20, 93, 549
initialization records, 441
default settings, 442
parameter display, 731, 732
input counts, 648
input flow control, 642
insert character, 172
insert mode
Telnet TN3270, 289
interactive protocol
defining, 85
interactive sessions, 249, 596
internet connections, 642
Internet security table. See IP security., 34
internet. See IP listings, 352
Internet-to-Ethernet address translation table, 47
interrupt settings
remote sessions, 146
Telnet, 269
Telnet ports, 268
IP addresses
autodiscovery, 354
broadcasts, 356
connection settings, 139
description of, 22
domain name servers, 359
DTFTP loading, 433
for outbound connections, 144
gateway router, 436
gateways, 372
host settings, 360
image file, 546
Kerberos, 427
load host, 433, 437
local, 202
local address range, 203
overriding, 462
parameter servers, 542
remote settings, 205, 206
RLOGIN, 581
rotary settings, 376
SecurID servers, 509
servers, 353
time servers, 515
XDM hosts, 305
Xremote font servers, 537
IP broadcast settings, 201
IP filters
destination ports, 150
protocol settings, 149
synchronization settings, 371
TCP SYN, 151
IP ICMP counters, 710, 711, 712
IP masks, 204
IP names
server settings, 374
IP ports
mapping to a rotary, 501
IP rotary
deleting entries, 45, 561
description of, 376
display rotary list, 713
IP routes, 46, 714, 715
adding, 377
current settings, 714
deleting, 565
deleting entries, 46
locally defined, 377
IP routing table size, 380
IP security, 138, 717
clearing table entries, 109
current table settings, 631
defining, 381
defining for ports, 138
deleting ports from database, 564
deleting table entries, 34, 562
disabling, 34
entry listings display, 716
table settings, 717
IP server
current settings, 704
current settings, 703
IP settings
current IP server, 705
IP SLIP, 140
IP SNMP settings display, 718, 719
IP subnet masks
autoconfigure feature, 389
server settings, 388
IP TCP
connect timer settings, 390
outbound address settings, 144
resequencing, 391
retransmit, 392
IP time to live, 68
IP-to-Ethernet translation, 47
IP traffic filters
destinations, 153
filtering criteria, 366
port settings, 147
protocols, 369
server destinations, 367
server settings, 366, 368
IPCP packets
displaying, 661
IPX addresses

destination nodes, 396
IPX filters, 395 - 401
IPX network numbers, 155, 402, 403
IPX packets, 158
IPX protocols, 404, 474
IPX RIP
broadcast timeout settings, 406
broadcasts, 405
broadcasts timer settings, 407
export filters, 37, 408
import filters, 38, 409
import routes, 50
network numbers, 37, 38
table size, 410
IPX route table, 157
exporting, 161
IPX routers, 158
IPX routes
deleting export routes, 49
IPX SAP
broadcast timeout settings, 412
broadcast timer settings, 212, 413
broadcasts, 210, 411
deleting export types, 52
deleting import types:, 54
deleting NetWare service types, 53
deleting service names and types, 51
export network settings, 414
export settings, 162
export types, 163, 415
import network settings, 416
import settings, 164
import types, 165, 417
network filters, 41
network numbers, 39
table sizes, 418
IPX traffic filters, 154
job numbers, 683, 684
keepalive timeouts, 214
keepalive timers
current settings, 629
IP TCP settings, 143
port settings, 213
server settings, 419
Kerberos
current settings display, 725 - 730
domain names, 427
error messages, 421
IP addresses, 427
master domain names, 423
outbound security, 185
password changes, 424, 425
password settings, 300
port connections, 426
port settings, 166
PPP PAP requests, 218
query limits, 428
realm names, 429
security settings, 430
server settings, 420
user verification, 430, 642
version 4, 420
version 5, 422
Kerberos 4 errors, 727, 728
Kerberos 5 errors, 729
keyboard characters
line editing function, 173
keymaps
adding entries, 525
copying to ports, 521
current listings, 652
current settings, 653
display current server status, 751
escape sequences, 167
overriding numeric only fields, 524
Telnet prefixes, 286
TN3270 ports, 167
keywords, 23
kickstart state, 255, 257
language settings, 290
LAT CONNECT PORT command, 553
LAT connections, 551
LAT messages, 431
LAT preferred service, 169
LAT protocol, 475
LAT service announcement, 455
LAT services, 60
port settings, 168
LAT solicits, 432
LCP echo reply timeout settings, 214
LCP echo requests, 213
LCP packets
current values, 657, 658
learned domain names, 365
limit settings
parameter servers, 468
limited view settings, 642
limited viewing settings, 170
limits
user sessions, 512
line editing character settings, 172
line editing characters
displaying, 607
line editor commands, 171
line editor settings, 642
line-feed characters, 271, 447, 448
LIST commands, 598, 599, 600
general information, 599
load file names
defining, 498

load files, 362
  current settings, 732
load images
  packet buffer sizes, 463
  retrieving from hosts, 546
loaddump settings, 441, 731, 732
loading image files, 345, 435, 440
loading information
  displaying, 609
local devices, 559
local switch character, 174
local time, 516
locally defined domain names, 32, 68
lock command, 444, 555
locked ports, 668
locked terminals, 285
logging
  port settings, 216
  Radius, 489
  Radius accounting, 487
  setting verbose priority levels, 532
  types of, 215
login password prompts, 576
login passwords, 188, 445
login prompts, 302, 446
login sequences, 125
login strings, 112
login time limits, 175
logins
  guests, 91
  UNIX hosts, 500
logons
  RLOGIN, 581
  welcome messages, 534
logout inactive ports, 133
logout or login strings
  defining, 112
logout ports, 121, 556
logout ports timer, 351
logout string
  defining, 112
logouts
  automatic, 99
  session disconnects, 330
loopback testing, 788 - 790
loss notification, 643
lost data notifications, 176
lpc command, 334
LPD counters, 334, 733, 734
LPD print queue settings, 447
LPD queues, 447, 735
  bypass offline ports, 450
  current server settings, 736
  deleting, 43
  status display, 738
lpq command, 334
lprm command, 334
MAC addresses
  displaying, 609
Macintosh users
  connecting to access servers, 89
magic number feature, 217
maintenance password, 451, 574, 575
MASK
  used as a keyword in commands, 152
  masks, 141, 204. See also IP masks.
  control characters, 196, 197
  current SLIP IP mask, 630
  SLIP ports, 244
memory
  current usage, 690
  server usage, 692
  session limits, 512
  texpool area size, 514
  usage with CCL scripts, 573
  usage with controlled ports, 331
  usage with VJ compression, 207
memory settings
  contents on server, 340
  menu files, 458
  nested menus, 459
  node limits, 460
  packet buffers, 463
menus, 643
  changing prompts, 454
  defining nested menu settings, 182
  deleting entries, 566
  deleting server menu items, 55
  designing for server, 452
  nested menu filenames, 458
  nested menu size, 459
  port settings, 177
  privileged nested menu feature, 224
  privileged ports, 223
  server menu settings, 739
message codes, 178, 643
messages
  APD, 320
  available LAT services, 318
  displaying at ports, 303
  length of identification messages, 349
  retransmit limits, 497
  server identification, 348
  user logons, 534
modems
  auto-answer mode, 331
  CCL scripts, 572
  control signal settings, 127, 179
  control signals, 114
  error messages, 496

outbound dialing, 251
outbound modem dialing, 250
signal settings, 243
speaker settings, 105, 639
MONITOR commands, 557, 598, 599, 600
general information, 599
multicast message strings
service settings, 539
multicast messages, 318, 540
multisessions, 180, 456
MX800 protocol, 476
naming conventions
domain names, 22
NCP LOAD command, 451
negotiating Telnet options, 596
nested menus, 182, 224
assigning highest level for ports, 183
displaying current value, 629
NetWare networks
deleting service types, 52 - 54
service types, 163, 415
NetWare services
IPX SAP import types, 417
next line character, 172
node address
for IPX networks, 155
node limits, 460
node names, 323, 609
nodes
connecting to services, 553
current status, 612, 617
hardware addresses, 609
IP addresses, 606
removing, 483, 484
status displays, 614, 615
noloss, 643
non-ANSI terminals, 598
Novell print servers
deleting, 58, 59
deleting entries, 571
mapping ports to, 535
services, 779
NULL character, 271
operational database changes, 327
option negotiations for Telnet, 273
out of sequence packets, 391
outbound address settings, 144
outbound security, 643
output counts, 648
output flow control, 643
overrun errors, 648
packet buffers
memory settings, 463
packet counters
IPCP display, 661
packet storage, 391
packet types
IPX, 404
IPX, 404
IPX filtering settings, 398
packets
ARAP, 635
defragmentation, 361
discard or accept, 152
out of sequence, 391
PAP
authentication requests, 218
password, 470
Kerberos authentication, 218
Radius authentication, 218
parameter files
displaying version numbers, 620
update attempt displays, 622
version numbers, 538
parameter servers, 464
adding to list, 542
bad parameter messages, 620
checking availability, 28
deleting, 35
deleting from database, 563
displaying current settings, 618 - 620
Ethernet addresses, 542
IP addresses, 542
maximum number of, 467
pathnames, 466
restransmit settings, 468
parity checking, 187
parity errors, 648
passall, 249
PASSALL sessions, 596
passcodes
SecurID, 504
SecurID authentication, 505
SecurID query limits, 508
password change services
Kerberos, 425
password prompts, 189
password protected service, 540
passwords
and remote connections, 574
ARAP, 322, 473
CHAP, 471
DECnet NCP TRIGGER, 451
default for privileged users, 595
default server login, 218, 445
disable login password, 445
disabling on port 0, 445
forgotten, 555
guest logins, 91
Kerberos, 300

locking terminals, 555
maximum attempts, 469
multisessions, 456
NCP LOAD commands, 451
PAP authentication, 218
port login, 188
port settings, 643
PPP PAP connections, 470
privileged commands, 472
privileged users, 594
RADIUS login, 194
remote console commands, 451
secure ports, 185
server default, 445, 472
server login, 445
service settings, 539
setting number of login attempts, 469
Telnet, 479
unlock terminals, 555
pasthru, 249
PASTHRU session, 597
pathnames for script files, 236
pause, 643
pause screens, 190
PCONSOLE utility, 535
permanent database changes, 327
Personal ID Number
for SecurID, 504
SecurID, 505
PIN numbers
SecurID, 504, 505
pinging gateways, 373
pinging Telnet destinations, 786
port 0, 445, 784
default setting, 640
security settings, 138
port access types, 82
port names
assigned by server, 181
port numbers
Kerberos server connections, 426
Telnet, 255
Telnet, 282
port security settings, 185
port settings
abort output setting, 247
APD, 84 - 88
AppleTalk zones, 94
ARAP, 89 - 94
assigning same port number to multiple ports, 277
authorized groups, 95
AUTOBAUD setting, 96
autoconnect, 97
autohangup, 99
autoprompting, 100
banner display before authentication, 304
baud rates, 83, 245
binary session mode, 249
break key action, 102
changing terminal type, 297
CHAP Radius authentication, 194
character sizes, 108
checking communications, 789, 790
clearing hung ports, 578
clearing IP security table entries, 109
command input buffer size, 110
connecting to LAT or Telnet, 64
controlled port strings, 645
copying port settings, 129
CSLIP compression, 136
current sessions, 665 - 671
current values, 636 - 644
DCD signal timeout, 114
dedicated services, 115, 116
dedicated services, 98
default port names, 181
default port numbers for Telnet, 281
deleting IP security entries, 564
destination port filters, 150
device names, 283
dial out settings, 121, 639
dialback settings, 119
dialback timeout setting, 120
dial up setting, 122
disabling IP security, 34
discard errors setting, 123
discard or accept packets, 152
disconnect, 543
displaying broadcast messages, 104
displaying current alternate characteristics, 627 - 630
displaying current values, 639, 640
download scripts, 236
DSRLOGOUT settings, 124
DSRWAIT, 125
DTRWAIT settings, 126
enabled by default, 641
enabling SLIP, 140
enabling SLIP autosend, 142
failure limits, 200
flow control, 186
flow control for input data, 134
forward session switching, 128
general information, 70
groups to display, 130
idle timeout, 132
inactivity action, 133
interrupt remote sessions, 146
IP addresses, 203

IP broadcast, 201
IP connections, 135
IP filter protocol, 149
IP filters, 147
IP masks, 204
IP remote address range, 206
IP security table entries, 650, 651
IPX SAP broadcasts, 210
keepalive timeout, 214
keepalive timer, 213
Kerberos authentication, 218
Kerberos password, 300
kickstart setting, 255, 257
LAT connections, 553
LAT preferred service, 169
length of break time, 103
limit the number of sessions, 242
line editor, 171
line editing characters, 608
local IP address, 202
login/logout settings, 112
login passwords, 188
login prompts, 302
login script files, 238
magic number feature, 217
mapping to Novell printer servers, 535
menu settings, 177
menus, 223
message displays, 178
messages, 303
modem speaker settings, 105
modified by VMS host, 231
multiple ports, 70
nested menus, 182, 183
notify if session is disconnected, 230
outbound Telnet connection, 144
parity, 187
password prompts, 189
pausing screens, 190
port counters, 646 - 649
PPP counters, 657, 658
PPP default settings, 199
PPP IP counters, 661
PPP IP settings, 659, 660
PPP IP status, 662
PPP option configuration requests, 198
PPP option negotiations, 192
PPP sessions, 191
PPP status, 663
PPP values, 654 - 656
preferred services, 222
prefix keymaps, 286
privilege nested menus feature, 224
privileges, 70, 594
Radius accounting, 487
RADIUS authentication, 219, 227, 228
rebooting with default parameters, 529
remote console ports, 574
remote IP addresses, 205
remote port numbers, 277
required for remote access, 89
resolve services feature, 232
resuming a connection, 111
return to previous session, 101
RLOGIN dedicated service, 233
RLOGIN preferred service, 234
script file commands diplay, 237
script server locations, 106
SecurID authentication, 239
security, 185, 240
services, 539
session mode, 117
session strings, 113
set to defaults, 296
SLIP IP masks, 244
stop bits, 246
summary display, 672 - 676
TCP keepalive timer, 143
TCP SYN filter, 151
Telnet 8bit, even parity, 274
Telnet attention character, 248
Telnet break type, 269
Telnet comport control, 250
Telnet comport display, 682
Telnet CSI escape sequences, 254
Telnet default location, 270
Telnet defaults, 784, 785
Telnet destination service, 255
Telnet display, 677 - 681
Telnet echo modes, 264
Telnet end of record, 284
Telnet erase keyboard character, 266
Telnet erase line character, 267
Telnet escape sequences, 254
Telnet insert mode, 289
Telnet interrupt character, 268
Telnet new line filtering, 272
Telnet new line sequences, 272
Telnet option negotiations, 273
Telnet port number, 255, 262
Telnet preferred service, 275
Telnet query character, 276
Telnet RS491 flow control, 278
Telnet synchronization character, 279
Telnet transmit characters, 293
Telnet urgent break, 295
Telnet userdata strings, 259, 260
terminal emulation for Telnet and RLOGIN, 280
testing connections, 788

TN3270 buffer size, 291
TN3270 keymap listings, 652, 653
TN3270 keymaps, 167, 521
TN3270 print screen, 82
TN3270 printer ports, 287
TN3270 scanners, 288
TN3270 screen attributes, 292
TN3270 screenmaps, 664
transmitting Telnet characters, 271
typeahead buffer size, 298
ULI, 299
user prompts, 225
username filtering, 301
VJ compression, 207
XDM host names, 305
XON send timer, 307
XREMOTE, 308
port status, 667
port types, 297
hardcopy, 172
ports
connecting to, 63
deleting Xprinter entries, 571
displaying port access status, 623
downloading scripts, 583
user names, 774 - 777
user names display, 774, 776
user status, 773
PPP
default settings, 199
IP counters, 661
IP settings, 659
IP settings, 660
PPP IP settings
current values, 662
PPP links, 155
PPP option configuration request packets, 198
PPP options, 192
PPP protocol, 477
PPP sessions, 191
PPP settings, 654 - 658
preferred services, 221, 222
description, 233
LAT ports, 169
Telnet, 275
prefix function keys
Telnet TN3270 sessions, 286
previous line character, 172
primary Internet gateway, 372
print screen
TN3270, 82
print servers
deleting Novell printer servers, 59
printcap file, 448
printer port settings
deleting XPRINTER ports, 58
preventing problems, 132
printer servers
mapping port to Novell, 535
Novell NetWare, 59
Novell printer servers, 778, 779
printer settings
deleting LPD queues, 43
device names, 287
displaying timeouts, 628
Xprinter timeout settings, 536
printers
80-column printing, 287
bypassing offline printers, 450
canceling print jobs, 43
clearing hung ports, 578
current status, 671
defining an end of message, 265
enable line feed characters, 448
enhancing performance of, 145
error messages, 496
LPD, 334
LPD counters, 733, 734
LPD queues, 447
Novell printer servers, 778, 779
parallel printer information, 670
port assignments, 287
TN3270 ports, 287
printing on a line printer, 249
priority levels
verbose accounting, 532
privilege levels, 20, 24
privileged menus, 223
privileges
port settings, 70, 594
prompts, 189
APD, 87
autoprompting, 100
changing login, 446
current settings, 630
default login prompt, 446
default settings, 225, 576
defining continue text for menus, 453
login password, 576
menus, 454
port login, 302
port settings, 225
protocols
APD defaults, 86
ARAP, 473
detecting automatically, 85
display current settings, 771, 772
enabling dump servers, 341
image file loading, 350, 439
initialization records, 438

IP filtering, 149
IPX, 474
IPX packet types, 404
LAT, 475
MX800, 476
PPP, 191, 477
SNMP, 478
Telnet, 479
TN3270, 480
RLOGIN, 581
types of, 149
Xprinter, 481
Xremote, 482
PURGE commands, 29, 31
PURGE DOMAIN command, 558
PURGE IP ROTARY command, 561
queries
XDM host, 306
query limits
Kerberos ID verification, 428
SecurID, 508
query types
XDM host, 306
queues, 541
deleting, 577
LAT connections, 683, 684
LPD, 735 - 738
port settings, 226
service settings, 539
setting limits, 485
quoting character, 172
Radius
accounting feature, 228
authentication, 227
CHAP challenge size, 488
current settings, 740, 741
enabling, 486
outbound security, 185
packet logging, 489
primary and secondary servers, 492
retry settings, 493
secrets settings, 491
solicitation feature, 229
UDP port setting, 490
Radius accounting, 487
displaying curent status, 631
RADIUS authentication, 219
realm names
Kerberos, 429
reassemble TCP/IP packets, 361
rebooting the server, 20, 549
rebooting with default parameters, 529
redisplay character, 173
REFRESH SERVER CCL NAME command, 572
reinitializing the server,66, 340, 549
remote, 574
remote access
default destination port, 277
required port settings, 89
remote accounting logging, 337
remote console command, 451
remote console facility, 575, 576
remote console ports, 784
remote console sessions
suspending, 784
remote modification feature
from VMS host, 231
remote SLIP addresses display, 628
report errors setting, 496
reset ports, 578
resetting counters, 793
resolve services feature, 232
resources
freeing up access, 132
restart timer settings, 220
resume command, 579
retries
SecurID server connections, 505
reverse video screens, 292
RFC2217(Telnet Com Port Control Options, 250
RING signals, 126
RIP
broadcasts and storage timers, 159 - 161
export filters, 37
import filters, 38
state command, 499
RLOGIN, 581
connecting to a UNIX host, 500
dedicated services, 233
displaying current settings, 630
preferred service, 234
terminal emulation, 280
transparent mode, 235
username restrictions, 234
ROM versions
display current, 771, 772
rotary
connections, 376
deleting entries, 561
description of, 45, 376
searching methods, 501
rotary groups, 68
roundrobin searches, 501
route tables
deleting, 49
routed, 335
router (RIP) table
size of, 410

table size, 410
router compatibility settings, 499
Router Information Protocol (RIP), 158, 405 - 410. See also RIP, 499
routing table
adding entries, 377
size of, 380
RS491
flow control, 278
rwho messages, 336
rwhod, 336
SAP broadcasts, 210
SAP export filters, 39
SAP import filters
deleting, 41
SAP service types, 39, 41
SAP table entries, 162, 414
scanner settings for TN3270, 288, 681
screen attributes, 292
TN3270 devices, 520
screenmaps
color modes, 523
current port settings, 664
TN3270 devices, 520
script logins
displaying current settings, 630
script servers, 502
current available hosts, 742
defining CCL names, 106
deleting from database, 56, 567
downloading scripts, 583
scripts
current settings, 694
deleting, 44
display commands at ports, 237
downloading, 236
filenames, 583
loading status, 668
login, 238
pathnames, 236
updating, 572
searching methods for IP ports, 501
secondary Internet gateway, 372
secrets
Radius, 491
secure status ports, 240
SecurID
authentication, 239, 503 - 509
current server settings, 743, 744
description of, 503
encryption mode, 507
maximum server retries, 505
outbound security, 185
passcodes and PIN numbers, 504
query limits, 508
server IP addresses, 509
time between prompts, 504
securing a terminal from other users, 555
security mask
defining, 138
security settings
banner displays before authentication, 304
current values, 650, 651
deleting ports, 36, 564
deleting security table entries, 562
group access, 510
Kerberos, 166, 420, 725, 726, 727, 728, 729, 730
Kerberos passwords, 300
Kerberos user verification, 430
locking ports, 444
port settings, 240
Radius CHAP challenge, 488
Radius servers, 492
RADIUS authentication, 227, 486
RADIUS solicitation feature, 229
SecurID authentication, 239, 503
SecurID current settings, 743, 744
remote and dynamic ports, 185
SecurID ports, 506
SecurID prompts, 504
servers, 381
security table entries, 34, 138, 717
exceptions for port 0, 138
server manager information
displaying, 609
server memory contents, 66
SERVER MENU display, 739
server name setting, 457
server number, 461
server parameters
displaying current settings, 609
server reinitialization, 66
server resources, 691
server settings
accounting logs, 317, 686, 687, 688, 689
adjusting response time, 329
APD, 319, 320
AppleTalk zones, 321
ARAP, 322, 473, 693
ARAP node names, 323
assigning server numbers, 461
auto-answer mode, 331
autoconfigure IP subnet masks, 389
autodiscovery, 354
broadcasts, 324
bypassing LPD ports, 450
CCL scripts, 694
changing login prompts, 446
changing time, 590

CHAP passwords, 471
checking parameter servers, 464
circuit timer settings, 329
continue menu prompts, 453
controlled ports, 331
copying flash cards, 325
crash dump, 340
creating rotary connections, 376
current status, 690 - 696, 746 - 749
dates, 339
default domain name suffixes, 357
default initialization parameters, 442
designing menus, 452
device table settings, 517, 518
domain names, 363, 374
DTFTP loading, 433
dump protocols, 341
error messages, 496
event logging, 343
file delimiters, 364, 434
fingerd daemon, 333
flash cards, 326
flash card updates, 345
formatting flash cards, 344
gateway IP address, 436
general information, 309
group access, 510, 511
heartbeat feature, 346
Help messages, 347
identifying servers, 348
image file loading protocols, 350
immediate ACK, 431
import service names and types, 417
inactive ports timer, 351
increment values, 375
initialization records, 438, 441
IP addresses, 353
IP addresses for domain name servers, 359
IP broadcast addresses, 356
IP counters, 706 - 708
IP filtering, 371
IP gateway addresses, 372
IP host addresses, 360
IP ICMP counters, 710 - 712
IP load file, 362
IP load host address, 437
IP rotary, 713
IP routes, 714, 715
IP security, 716, 717
IP SNMP, 718, 719
IP rotary entries, 45
IP route entries, 46, 565
IP routes, 377
IP routing table, 380
IP security, 381
IP subnet masks, 388
IP TCP connect timer, 390
IP traffic filtering, 366, 368
IPX destination criteria, 397
IPX filtering, 395 - 400
IPX internal network numbers, 402
IPX network numbers, 403
IPX protocol, 474
IPX RIP broadcasts, 405, 407
IPX RIP export filters, 408
IPX RIP import filters, 409
IPX RIP table size, 410
IPX SAP broadcasts, 411 - 413
IPX SAP exporting service names and types, 414
IPX SAP import service names and types, 415,
IPX SAP table size, 418
IPX source network, 399
IPX traffic filtering, 401
keepalive timer, 419
Kerberos, 420
Kerberos 5, 422
Kerberos display, 725 -730
Kerberos domain names, 427
Kerberos error messages, 421
Kerberos IP addresses, 427
Kerberos master, 423
Kerberos password changes, 424, 425
Kerberos port numbers, 426
Kerberos query limit, 428
Kerberos realm names, 429
Kerberos security, 430
LAT protocol, 475
LAT solicits, 432
load filenames, 435, 498
loaddump display, 731, 732
loading image files, 440
LPD counters display, 733
LPD daemon, 334
LPD print queues, 447
LPD queues, 738
menu items, 55
maintenance passwords, 451
maximum parameter servers, 467
maximum user sessions, 512
memory contents, 340
memory settings for nested menu, 459
menu setting display, 739
message sizes, 349
multicast messages, 318
multicast timers, 455
multisessions, 456
MX800 protocol, 476
nested menu filenames, 458

node limits, 460
out of sequence packets, 391
overriding IP addresses, 462
packet discarded timer, 394
parameter server pathnames, 466
parameter server retransmit, 468
password attempts, 469
port locking, 444
PPP PAP passwords, 470
PPP protocol, 477
privileged passwords, 472
query limits for SecurID, 508
queue limits, 485
Radius, 492
Radius accounting, 487
Radius authentication, 486, 740, 741
Radius authentication timeout, 494
Radius CHAP challenge size, 488
Radius logging, 489
Radius retry settings, 493
Radius secrets, 491
Radius UDP ports, 490
reassemble packets, 361
rebooting, 549
rebooting with default parameters, 529
reinitialization, 340
reliable accounting sessions, 495
removing LAT nodes, 483
removing nodes, 484
report errors. See also error messages., 496
retransmit feature, 392
retransmit limits, 497
RLOGIN, 500
rotary roundrobin, 501
routed daemon, 335
routing information, 499
rwhod daemon, 336
screen colors, 523
script servers, 502
SecurID, 509, 743, 744
SecurID authentication, 503
SecurID encryption mode, 507
SecurID prompts, 504
server counters, 699 - 702
server IP settings, 703 - 705
SNMP authentication traps, 382
SNMP community, 386
SNMP community name, 383, 385
SNMP contact name/location, 387
SNMP counters, 720, 721, 722
SNMP protocol, 478
specify database updates, 327
status message display, 443
summary display, 750
switching gateways, 373
syslogd daemon, 337
TCP ACK packets, 513
TCP counters, 708
TCP port starting base, 375
Telnet protocol, 479
textpool size, 514
time, 339
time servers, 515
time-to-live translation table entries, 393
TN3270 device tables, 568
TN3270 devices, 752, 753, 754
TN3270 keymap entries, 525
TN3270 protocol, 480
TN3270 screen attributes, 520
TN3270 screen colors, 523
TN3270 screenmaps, 520
TN3270 translation tables, 47, 527, 755, 756
translation table display, 723, 724
UDP counters, 709
UDP port for Radius accounting, 487
UDP ports SecurID, 506
ULI, 528
unique server names, 457
userdata delays, 530
verbose accounting, 531
verbose priority levels, 532
version numbers for parameter files, 538
welcome messages, 534
Xprinter protocol, 481
Xprinter timeouts, 536
Xremote, 482, , 537, 757, 758
Service Advertising Protocol (SAP), 210 - 212, 411 - 413, 418
service settings
connections, 539
identification, 539
passwords, 539
ports, 539
queue, 539
service types, 51 - 54
deleting, 52, 53
NetWare, 54
SAP, 39, 41, 414, 416
service names
displaying, 604
services
current settings, 759 - 766
current status, 615
deleting, 57, 570
SERVICES CHARACTERISTICS display:, 760
session modes, 241, , 630, 768
Telnet binary, 249
session numbers, 544

session settings, 118
session types
  defining, 596
  default port numbers for TN3270, 281
sessions, 545
  autohangup, 99
  background mode, 174
  changing connection strings, 113
  connecting, 25
  console port logouts, 330
  creating between terminal and Telnet, 780 - 783
  current port session, 665 - 671
  current service session settings, 767 - 770
  DEC terminal support, 180
  defining port login/logout strings, 113
  definining initial settings, 117
  disconnect, 543, 556
  displaying informational messages, 303
  forwards command, 544
  interactive, 241
  INTERACTIVE_NOIAC, 241
  keyboard settings, 128
  LAT connections, 551
  limiting the number of, 242
  maximum number, 242
  maximum users, 512
  notification of disconnect, 230
  PASSALL, 241
  PASTHRU, 241
  PPP, 191
  preventing remote users, 371
  resuming, 579
  retransmit limits, 497
  RLOGIN, 235
  selecting next, 544
  sesstion types, 596
  starting, 60, 61, 62
  switching to next session, 128
  Telnet default port numbers, 282
  Telnet query character, 276
  Telnet settings, 268
  Telnet teminal emulation, 280
  terminal types, 280
  timeout displays, 628
  TN3270 overriding numeric-only fields, 524
  TN3270 terminal types, 283
  transmitting Telnet characters, 271
  TRANSPARENT, 241
  using ASCII control characters, 195
  VJ compression, 208
set commands, 67
  general information, 584
set port commands
  general information, 70
SHOW commands, 598 - 600
show unit, 771, 772
SHOWKEYS status key
  TN3270 terminal emulation, 167
signal check setting, 243
SLIP, 140, 141
  current packet status, 649
  address display, 628
  autosending, 142
  IP MASK setting, 244
  links, 136
  protocol, 140
SNAP type packets, 404
SNMP
  authentication traps, 382
  client number, 384
  client settings, 383
  community name, 385
  counters, 720, 721, 722
  display settings, 718, 719
  protocol, 478
  Set or Get client, 384
  Set or Get community name, 383 - 386
  system contact/location, 387
  trap clients, 383, 384
  trap community name, 386
software loading, 440
solicitation feature
  RADIUS, 229
solicits setting, 432
speed
  baud rates, 83
state
  displaying server manager information, 609
static displays, 598
statistics
  current node information, 612
  port counters, 646 - 649
status, 667
  alternate server status, 690 - 692
  current port session, 665 - 671
  current port settings, 773
  current port summary, 672 - 676
  current server settings display, 746 - 749
  current service displays, 615
  current services settings, 762 - 764
  current node status, 612
  current parameters, 621
  LPD queues, 738
  PPP IP settings, 662
  PPP settings, 663
status messages, 443
stop bits, 246

stop bits used
displaying current value, 629
stopping image updates, 547
subnet masks, 388
summary
display current services settings, 765, 766
switch characters, 249, 596
switching between sessions, 25, 544
SYN bit
using for traffic filtering, 371
synchronization
IP filters, 147
synchronization bit settings, 371
synchronize character, 279
syslogd, 337
table size
IPX SAP, 418
target port, 63
TCP accounting sessions, 495
TCP ACK packets, 513
TCP counters, 708
TCP port starting base
server settings, 375
TCP window size
displaying current settings, 629
TCP/IP
session window size, 145
TCP/IP destinations, 135
Telnet
abort output character, 247
attention character, 248
binary option, 596
binary session mode, 249
break lengths, 103, 639
break sequences, 295
break type, 269
buffer size, 291
buffered transmissions, 293
com port control options, 250
command characters, 249, 596
comport settings, 682
connect command, 780, 781
connection timers, 390
connect port command, 782, 783
current port settings, 677
dedicated service, 255, 259, 260
default characters, 678
default location, 270
default port numbers, 282
default port settings, 262, 785
destinations, 275
echo modes, 264
end-of-record messages, 265
erase keystroke character, 266
erase line character, 267
escape sequences, 254
interactive mode, 249
interrupt character, 268
interrupt settings, 269
newline setting, 271, 272
option negotiations, 273
PASS8D settings, 274
pinging, 786
port numbers, 22, 61, 259, 262
port settings, 679 - 681
prefix keymaps, 286
protocol, 479
query settings, 276
resolve services, 232
screen attributes, 292
sessions, 596
synchronization character, 279
TN3270 EOR setting, 284
TN3270 error locks, 285
TN3270 scanner settings, 288
TN3270 translation tables, 290
TN3270 XTDATTRS settings, 292
transmit settings, 293
user data strings, 255, 259, 260
terminal emulation
Telnet, RLOGIN, 280
TN3270 sessions, 283
terminal locking, 285
terminal types
changing, 297
terminals
securing, 555
test loop command, 787
test port command, 788
test service command, 789, 790
testing communications, 786
textpool size, 514
time servers, 515
time settings
resetting after reboot, 339
servers, 590
time zones, 516
time-to-live settings, 68, 365, 394, 712
domain names, 365
limits, 377
time zones, 516
timeout settings
APD, 88, 639
DCD port signals, 114
gateway pinging status, 373
idle time, 133
IP TCP retransmit, 392
IPX RIP broadcasts, 406
IPX SAP broadcasts, 211, 412
keepalive, 214

port dialbacks, 120
port idle time, 132
Radius server, 494
server IPX RIP broadcasts, 159
Xprinter, 536
timer settings
announcement displays, 455
CHAP challenge, 193
displaying keepalive timer, 629
inactive sessions, 351
inactivity logout, 642
IP gateways, 377
IP TCP KEEPALIVE, 143
IPX RIP broadcasts, 407
IPX SAP broadcasts, 212
keepalive, 419
LCP echo requests, 213
parameter servers, 468
restarting packet requests, 220
RIP port information, 160
service node performance, 329
Telnet connections, 390
Telnet idletime, 293
Telnet transmissions, 293
XON sends, 307
TN3270
adding entries to TN3270 keymaps, 525
alternate keymapping, 521
deleting devices from TN3270 device tables, 568
device settings, 517, 751 - 754
extended 7-color mode, 523
insert mode, 289
keymaps, 167
port keymapping, 521
print screen, 82
protocol, 480
translation tables, 527, 755, 756
scanner feature, 681
XTDATTRS, 523
overriding numeric-only fields, 524
screenmap settings, 664
TN3270 sessions
default port numbers, 281
end of record, 284
error locks, 285
printing, 287
terminal emulation, 283
traffic
importing routes, 157
traffic filters
IPX, 154
translation tables
deleting, 47, 569
modifying TN3270 entries, 527
server display, 723, 724
time-to-live settings, 393
TN3270, 290
transparency, 596
transparent mode
RLOGIN, 235
TSM scripts, 445, 496
TTL. *See* also time to live. 68, 365, 606, 702
typeahead, 184, 291, 294, 298, 630
UDP
counters, 709
SecurID ports, 506
Radius accounting, 487
Radius, 490
ULI
enabling, 791
port settings, 299
server settings, 528
underline on screens, 292
UNIT display, 771, 772
universal time
time settings, 516
UNIX
aliases, 24
UNIX hosts
connecting to, 500
logging on, 500
UNIX like user interface. See ULI., 299
unlocking a terminal, 555
urgent breaks, 295
USENGLSH translation table, 569
user names
current port status, 774, 775, 776, 777
userdata strings, 259, 260
ASCII characters, 258
Telnet, 255
username filtering, 301
username prompt setting, 302
username restrictions
RLOGIN, 234
users display, 774
Van Jacobson compression, 136, 207
verbose accounting, 215, 531, 686
verbose priority
server settings, 532
version numbers, 771, 772
parameter files, 538, 620
VMS host
changing port settings, 231
welcome banner
display before authentication, 304
welcome messages, 534
wildcard characters, 604, 605
window size
TCP/IP sessions, 145

XCONNECT, 792
XDM
displaying current settings, 629, 630
font servers, 537
host settings, 305, 792
query types, 306
XREMOTE settings, 308
XON timer settings, 307
XON/XOFF flow control, 186, 249, 596
XPRINTER
deleting, 58, 571
protocol, 481
settings, 535, 778, 779
Xremote
font servers, 537
IP addresses, 537
protocol, 482
settings, 308, 757, 758
XTDATTRS feature, 292
zero counters command, 793
ZModem settings, 235
zone names
AppleTalk, 94