



Total Control® 1000 Enhanced Data System

Access Router Card
Command Line Reference
Release 4.5
Part Number 10048398



Total Control® 1000 Enhanced Data System

Access Router Card
Command Line Reference
Release 4.5
Part Number 10048398

Copyright © 2002, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

UNITED STATES GOVERNMENT LEGENDS:

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

United States Government Legend: All technical data and computer software is commercial in nature and developed solely at private expense. Software is delivered as Commercial Computer Software as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFARS 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo, Boundary Routing, EtherDisk, EtherLink, EtherLink II, LANplex, LinkBuilder, Net Age, NETBuilder, NETBuilder II, OfficeConnect, Parallel Tasking, SmartAgent, SuperStack, TokenDisk, TokenLink, Transcend, and ViewBuilder are registered trademarks of 3Com Corporation. ATMLink, AutoLink, CoreBuilder, DynamicAccess, FDDILink, FMS, NetProbe, and PACE are trademarks of 3Com Corporation. 3ComFacts is a service mark of 3Com Corporation.

Artisoft and LANtastic are registered trademarks of Artisoft, Inc. Banyan and VINES are registered trademarks of Banyan Systems Incorporated. CompuServe is a registered trademark of CompuServe, Inc. DEC and PATHWORKS are registered trademarks of Digital Equipment Corporation. Intel and Pentium are registered trademarks of Intel Corporation. AIX, AT, IBM, NetView, and OS/2 are registered trademarks and Warp is a trademark of International Business Machines Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. PictureTel is a registered trademark of PictureTel Corporation. UNIX is a registered trademark of X/Open Company, Ltd. in the United States and other countries.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

CONTENTS

ABOUT THIS GUIDE

Conventions	xxxiii
Related Documentation	xxxiv
Total Control 1000 Enhanced Data System	xxxiv
Total Control HiPer System	xxxiv
Contacting Customer Service	xxxvii

1 USING THE COMMAND LINE INTERFACE

Overview	39
Accessing the Command Line Interface	39
Command Format	40
Parameters	40
Syntax, Examples, and Related Commands	41
Entering Commands	41
Using Control Characters	41
Abbreviation and Command Completion	42
Help	42
Additional Conventions	43
Network Address Formats	43
Interface Ranges	44
Names	44
Interface Names	44
Users	45
Default User	45
Command Language Structure	45
Command Line Interface Conventions	46

2 MANAGEMENT COMMANDS

Command Features	51
Command Line Edit	51
Command Retrieval	52
Positional Help	52
Command Completion	52
Output Pause	52
Ending a Process	52
Administrative Commands	53
help	53
history	53
kill	54
reboot	54
save all	54



save configuration	55
Date and Time Commands	55
set date	55
set time	56
set timezone.....	56
list timezone.....	57
show date	57
show time	57
Bulk File Commands	58
set bulk_file.....	58
show bulk_file	58
Chat Script Commands.....	58
add chat_script.....	58
verify chat_script.....	59
delete chat_script	60
list chat_scripts	60
show chat_script.....	61
Page Break Commands.....	61
enable command global_terminal_settings_page_breaks	61
disable command global_terminal_settings_page_breaks.....	62
enable command local_terminal_settings_page_breaks.....	62
disable command local_terminal_settings_page_breaks	63
Set Commands	63
set command.....	63
set system.....	64
show all configuration output.....	66
do	66
cfp_delay_command.....	67
set board command_line_parameters	67
set bootrom boot interface	67
set bootrom config.....	67
set bootrom ip interface	68
CLI Exit Commands.....	69
quit	69
logout	69
leave.....	69
EEPROM	70
delete board crashdump	70
show board crashdump	70
disable system reset_eeprom	70
enable system reset_eeprom.....	71
Event Logging Commands	71
add syslog	71
delete syslog.....	72
disable icmp logging.....	73
disable syslog event_log.....	73
enable syslog event_log.....	73
reset syslog event_log.....	73

enable icmp logging.....	74
list syslogs	74
set facility.....	75
show events.....	75
set syslog	76
set syslog_format	77
show syslog	77
show syslog_format	77
Event Commands.....	78
disable critical_events_to_flash.....	78
enable critical_events_to_flash	78
hide events	79
list critical events.....	79
show events.....	79
IP Network Commands.....	80
delete ip source route.....	80
list ip addresses	80
list ip defaultroute	81
reconfigure ip network.....	81
Monitoring Protocols.....	82
monitor protocol.....	82
Show All Commands.....	83
show all configuration settings.....	83
show all active interfaces.....	83
show all connections.....	83
show all filters.....	84
show all interfaces	84
show all ip networks	84
show all ipx networks.....	84
show all l2tp tunnels	84
show all lan interfaces.....	84
show all networks.....	84
show all ospf areas.....	85
show all ospf interfaces.....	85
show all sessions.....	85
show all switched interfaces.....	85
show all users	85
show all vpn.....	86
show all vtp tunnels	86
Show Commands.....	87
show board command_line_parameters	87
show board settings.....	87
show bootrom settings.....	87
show command settings	88
show configuration settings	88
show cpu utilization	89
show date.....	89
show file	89

show maximum_local_users.....	89
show memory.....	90
show memory utilization.....	90
show network	91
show packet_logging.....	91
show remote user.....	91
show session	92
show system.....	93
Statistics	93
show statistics	93
reset	95
reset statistics	96
Session Commands.....	97
list sessions.....	97
list sessions counters.....	97
TCP Commands.....	97
show tcp counters	97
PPP Commands.....	98
show ppp on interface <slot:x/mod:y> counters.....	98
UDP Commands	99
list udp listeners.....	99
show udp counters.....	99
VTP Commands	100
show vtp	100
Accounting.....	101
show accounting counters.....	101
show accounting server_group [a b] counters	101
ATM Commands.....	102
show atm counters [ds3:x e3:x atmcell:x]	102
Authentication Commands	102
show authentication settings.....	102
show authentication counters.....	103
show authentication server_status	104
Connection Commands	104
show connection settings	104
show connection counters.....	105
DNS Commands	105
show dns counters.....	105
Frame Relay Commands.....	107
show frame_relay interface <interface_name> counters.....	107
show frame_relay interface <interface_name> lmi statistics	108
show frame_relay pvc <pvc_name> counters.....	109
show datalink frame_relay interface <interface_name> counters	111
show datalink frame_relay interface <interface name> lmi statistics.....	112
Chassis Commands.....	113
list chassis.....	113
show chassis slot <slot number>.....	113
show nmc status.....	113

File Commands	113
delete configuration	113
delete file	114
edit	114
show critical_event settings	114
copy file	114
list files	115
rename file	115
show bulk_file	115
Network Commands	115
list network	115
show network <name> settings	116
show network <name> counters	116
Policy Commands	116
list policy	116
Processes and Facilities Commands	116
list facilities	116
list processes	116
Routing Table Commands	117
list rtab preferred	117
GRE Commands	117
show gre counters	117
Health Trap Commands	118
disable health_trap	118
enable health_trap	118
set health_trap interval	118
show health_trap	118
ICMP Commands	118
show icmp counters	118
Interface Commands	120
show interface <interface_name> counters	120
IP Network Commands	121
show ip counters	121
show ip rip counters	122
IPX Network Commands	122
show ipx counters	122
show ipx network <network_name> counters	123
show ipx rip counters	124
show ipx sap counters	124
L2TP Tunnel Commands	124
show l2tp counters	124
NMC Commands	126
show nmc counters	126
OSPF Commands	126
show ospf area <area_id> counters	126
show ospf global counters	127
Ping	128
show ping row <row_number> counters	128



show ping server <host name or IP address> counters	129
PPPoE Commands.....	129
show pppoe [counters settings].....	129
PPTP Commands.....	129
show pptp counters.....	129
RADIUS.....	131
show radius resource_management counters.....	131
RSH Process Commands.....	132
show rshd counters	132
SNMP Commands.....	132
show snmp counters.....	132
Tunnel Switch (L2TP & PPTP)	133
show tunnel switch_counters.....	133
TFTP.....	134
show tftp request	134
list tftp requests.....	134
Packet Bus Datagrams.....	135
list pbus datagrams.....	135
Traceroute.....	135
traceroute.....	135
list traceroute	137
list traceroute row <number> hops.....	138
delete traceroute row	138
set traceroute maximum_rows.....	138
show traceroute settings.....	139
show traceroute row <number> settings	139
Telnet Commands.....	140
telnet.....	140
telnet <IP_name or address> TCP_port <number>	140
Dial-in User Telnet Commands	141
connect	141
exit.....	141
help.....	141
logout	141
manage.....	141
rlogin.....	142
telnet.....	142
set telnet admin_banner_file.....	142
Telnet Commands (Console Port)	142
close.....	142
help.....	143
send	143
set escape.....	143
status	143
Other Telnet Related Commands.....	144
add telnet client.....	144
delete telnet client.....	144
disable telnet disconnect_message.....	144

enable telnet disconnect_message	144
enable telnet.....	145
disable telnet	145
list telnet clients	146
show telnet settings	146
User Commands.....	147
add user.....	147
delete user	148
disable user.....	148
disconnect user	149
enable user	149
list users.....	150
Set User Commands.....	150
set user	150
set dialout user	153
set dialout user <user name> site.....	154
set framed_route user	156
set login user	156
show user	157
set maximum_local_users.....	158
Network User Commands	158
set network user	158
set network user <user name> igmp	159
set network user <name> ip.....	160
set network user <user name> ipx.....	162
set network user <user name> ppp.....	163
set network user <user_name> ppp_source_ip_filter [enabled disabled]	165
Tunnel User Commands.....	165
set tunnel user	165
Address Pool User Commands.....	166
add address_pool user.....	166
delete address_pool user.....	167
Security Option Commands.....	167
disable security_option remote_user_ administration	167
enable security_option remote_user_ administration	167
TCP	168
disable tcp keepalives	168
disable tcp nagle_algorithm	168
enable tcp keepalives	168
enable tcp nagle_algorithm.....	169
list tcp connections	169
set clearTCP connect_message	170
set tcp keepalive_interval	171
set tcp maximum_connections	171
show clearTCP	171
show tcp.....	172

3 HOST AND SERVER COMMANDS

DHCP	173
set dhcp_proxy	173
show dhcp_proxy settings.....	174
list dhcp_proxy leases	174
show dhcp_proxy counters	175
Login	175
add login_host.....	175
delete login_host preference.....	176
add login_table.....	177
list login_table	177
delete login_table	178
disable prompting single_level	178
disable rlogin escape.....	178
enable prompting single_level.....	179
enable rlogin escape.....	179
list login_hosts.....	179
list login_sessions.....	180
resolve name	180
rlogin.....	181
set login_host preference.....	181
set login_table <name>	182
show prompting	183
Ping	183
add ping service_loss_system	183
delete ping row	184
delete ping service_loss_system	185
disable ping service_loss_system	185
enable ping service_loss_system.....	185
list ping service_loss_systems	185
list ping systems.....	186
ping.....	187
set ping maximum_rows.....	188
set ping service_loss_system	189
show ping settings.....	189
show ping row	190
show ping server settings.....	190
show ping server <host name or IP_address> settings.....	191
RSHD	191
add rshd clients	191
delete rshd clients.....	191
list rshd clients.....	192
SNMP	192
add snmp community.....	192
add snmp community_pool	193
add snmp trap_community.....	194
add snmp trap_community_pool	195
delete snmp community	195

delete snmp community_pool	196
delete snmp trap_community	196
delete snmp trap_community_pool	196
disable link_traps interface	197
disable security_option snmp user_access	197
disable snmp authentication traps	197
enable link_traps interface	198
enable security_option snmp user_access	198
enable snmp authentication traps	198
list snmp communities	199
list snmp community_pools	199
list snmp trap_communities	200
list snmp trap_community_pools	200
set snmp community	201
set snmp trap_community	202
show snmp settings	202
show snmp community_pool	203
show snmp trap_community_pool	203
TFTP	203
add tftp client	203
add tftp request	204
delete tftp client	205
delete tftp request	205
disable tftp request	205
enable tftp request	206
list tftp clients	206
set tftp request	206
tftp	207

4 REMOTE ACCESS COMMANDS

Network Dial-In Access	209
add ip pool	209
add mpip client	211
add mpip server	212
list ip aggregate_routes	212
list mpip bundles	213
list mpip clients	213
list mpip links	213
list mpip locallinks	214
list mpip servers	214
set connection	214
set ip pool	216
set ipx system	217
set ppp	219
set mpip	221
set mpip client	221
set mpip server	222

show mpip settings.....	223
NTP	223
disable ntp.....	223
enable ntp.....	223
set ntp.....	224
show ntp settings	225
Network Dial-Out Access: Dialout	225
dial.....	225
dialout l2tp.....	225
dialout pptp.....	226
set dialout user	226
Modem Groups	227
add modem_group.....	227
assign interfaces	228
delete modem_group	229
disable modem_group	229
list modem_groups.....	230
show modem_group	230
Network Service.....	231
add network service.....	231
list network services.....	234
set network service.....	235
delete network service.....	236
disable network service.....	236
enable network service	237
list available servers.....	237
SLIP	237
disable slip offloading	237
enable slip offloading	238
set slip session_start_message.....	238
show slip settings	239
Cross Connect Commands.....	239
add cross_connect.....	239
delete cross_connect	240
enable cross_connect.....	240
show cross_connect.....	240
list cross_connect.....	241

5 INTERFACE AND MODEM COMMANDS

DS1 Interface.....	243
assign interfaces	243
add logical_ds1 interface	243
delete logical_ds1 interface.....	244
disable interface	244
enable interface.....	244
hangup interface	245
list active interfaces.....	245

list ds_one interfaces	245
list connections	246
list interfaces	247
list ip interface_block	247
list switched interfaces	248
list sync interfaces	248
set ds1 interface.....	249
set logical_ds1 interface	251
show ds1 interface	251
set switched interface	252
set sync interface	258
show bootrom ip interface	260
show ds1 interface <physical_interface_name> ch_map.....	261
show ds1 interface <physical_interface_name> current_tbl	262
show ds1 interface <physical_interface_name> fend_current_tbl	263
show ds1 interface <physical_interface_name> fend_interval_tbl	264
show ds1 interface <physical_interface_name> fend_total_tbl	264
show ds1 interface <physical_interface_name> interval_tbl.....	265
show ds1 interface <physical_interface_name> total_tbl	266
show interface <interface name> settings	266
show logical_ds1 interface <logical_interface_name> ch_map	268
unassign interface <interface_name_list> modem_group <group_name>	269
Call Reject Code Commands	269
enable call reject_code	269
disable call reject_code.....	269
show call reject_code status	270
Modem Auto-Answer Commands	270
disable auto_answer	270
enable auto_answer	270
show auto_answer	271
Modem Chassis Slot Commands	271
set chassis slot.....	271
set chassis slot <slot_list> console [no yes].....	272
enable chassis contiguous_modem_naming	272
disable chassis contiguous_modem_naming.....	273
Initialization Script Commands	273
add init_script	273
delete init_script.....	274
list init_scripts	274
set init_script.....	275
Modem_group	275
enable modem_group.....	275
hangup modem_group	276
set modem_group.....	276
Network Management Card Commands	282
disable nmc chassis_awareness.....	282
disable nmc dsa_idle_rebalancing.....	282
disable nmc dynamic_slot_assignment	283

disable nmc snmp_forwarding	283
enable nmc chassis_awareness	283
enable nmc dsa_idle_rebalancing	284
enable nmc snmp_forwarding	284
enable nmc dynamic_slot_assignment	284
show nmc settings	286
PBUS	286
list pbus sessions	286
list pbus traps	287
show pbus settings	287
show sync interface	287
Datalink Frame Relay	288
set datalink frame_relay interface	288
show datalink frame_relay interface <interface_name> counters	288
show datalink frame_relay interface <interface_name> lmi statistics	289
RS232	290
show rs232 interface	290
TAP	291
add tap interface	291
add tap next	293
add tap user	294
delete tap	295
list tap	295
set tap id	296
delete tap id	296
set tap user	297

6 ROUTING COMMANDS

Address Resolution Protocol Commands	299
add atm_arp_server	299
add ip arp address <IP address> access_mac_address <MAC address> interface <interface name>	300
add ip arp address <IP address> state [private public]	301
arp	301
clear arp_cache	301
delete atm_arp_server	302
delete ip arp address <IP address> interface <interface name>	302
disable atm_arp_server	303
enable atm_arp_server	303
list ip arp	304
show atm_arp_server	304
Inverse Address Resolution Protocol Commands	305
add ip invarp <IP address> type [dynamic static]	305
delete ip invarp	305
show ip invarp	305
list ip invarp network	306
invarp ptmp_pvc_group	306
invarp pvc	306

Asynchronous Transfer Mode	307
add atm1483 pvc	307
add atm1577 pvc	308
delete atm1483 pvc	309
delete atm1577 pvc	309
disable atm1483 pvc	309
disable atm1577 pvc	310
disable atmsig	310
list atm1483 pvcs	310
list atm1577 pvcs	311
set atm options	311
set atm_address network	312
show atm1483 pvc <name> settings	312
show atm1577 pvc <name> settings	313
show atmcfg	313
add ip defaultroute gateway	313
add ip network	314
add ip route	316
add framed_route user	317
add ip source route <IP or net addr> gateway <IP name or addr> metric <metric>	317
add ipx network	318
add ipx route	319
add ipx service	320
delete ip defaultroute gateway	322
delete ip network	322
delete ip pool	323
delete ip route	323
delete ip source route	324
delete ipx network	324
delete ipx route	324
delete ipx service	325
delete ipx service_all	325
disable ip	325
disable ip address_pool_filtering	326
disable ip address_pool_round_robin	327
disable ip forwarding	327
disable ip iea_force_nexthop_route	327
disable ip iea_next_hop_routing	328
disable ip multicast_heartbeat	328
disable ip network	329
disable ip proxy_arp_all_dialin	329
disable ip rip	329
disable ip routing	330
disable ip send_unsolicited_arp	330
disable ip send_host_unreach_for_pool	330
disable ip source_address_filter	331
disable ip static_remote_routes	331
disable ipx network	331

disable ipx rip network.....	332
disable ipx sap network	332
enable ip	333
enable ip address_pool_filtering.....	334
enable ip address_pool_round_robin.....	334
enable ip forwarding	334
enable ip ie_force_nexthop_route	335
enable ip ie_next_hop_routing.....	335
enable ip multicast_heartbeat	335
enable ip network.....	336
enable ip proxy_arp_all_dialin	336
enable ip rip	337
enable ip routing	337
enable ip send_unsolicited_arp	337
enable ip source_address_filter	338
enable ip static_remote_routes	338
enable ipx network	339
enable ipx rip network	339
enable ipx sap network.....	339
list ip networks	340
list ip pools	340
list ip routes.....	341
list ip source routes.....	342
list ip static_arp.....	342
list ipx networks.....	343
list ipx routes	343
list ipx services	344
list ipx static routes	345
list lan interfaces.....	345
list ppp	345
set ip application_source_address	346
set ip arp address.....	347
set ip defaultroute gateway	347
set ip defaultroute metric.....	347
set ip network <name>	348
set ip route <IP_hostname or network address>.....	351
set ip routing	352
set ip source_based_routing	353
set ip source route	353
set ip unnumbered_link local_address <IP address>	354
set ipx network.....	355
show ip settings.....	357
show ip network settings.....	358
show ip network <network_name> settings	359
show ip routing settings	360
show ip source_based_routing <interface_name>.....	360
show ipx.....	360
show ipx network <network name> settings	361

show ipx rip settings	363
show ipx sap settings	363
add cross_connect.....	363
enable cross_connect	364
disable cross_connect.....	364
list cross_connect	364
show cross_connect	364
DNS	365
add dns host	365
add dns server.....	365
delete dns cache	366
delete dns host	366
delete dns ncache	367
delete dns server preference.....	367
disable dns host_rotation	367
disable dns round_robin	367
enable dns host_rotation.....	368
enable dns round_robin	368
host <IP_host_name>.....	369
list dns cache	369
list dnis_connections	370
list dns hosts	370
list dns ncache	371
list dns servers.....	371
set dns	372
set dns server preference.....	373
show dns settings	373
show dns cache	374
show dns ncache	375
Frame Relay.....	375
add frame_relay pvc.....	375
add frame_relay ptmp_pvc_group.....	376
list frame_relay ptmp_pvc_group.....	376
show frame_relay ptmp_pvc_group <net name> counters.....	376
show frame_relay ptmp_pvc_group <net name> settings.....	377
show frame_relay pvc <net name> settings.....	377
show frame_relay pvc <net name> counters	378
add datalink frame_relay interface <interface_name>	378
delete datalink frame_relay interface	379
delete frame_relay pvc	379
add framed_route user.....	379
delete framed_route user	379
disable frame_relay pvc	380
disable datalink frame_relay interface.....	380
enable datalink frame_relay interface	380
enable frame_relay pvc.....	381
list frame_relay.....	381
set frame_relay conformance	382



set frame_relay traps	382
set frame_relay trap_min_interval	382
set frame_relay interface.....	383
set frame_relay pvc <pvc_name>	385
show frame_relay interface <interface_name> settings	386
show frame_relay pvc <pvc_name> settings	388
show frame_relay stack	389
show datalink frame_relay interface <interface_name> settings.....	390
ICMP	391
disable icmp router_advertise	391
enable icmp router_advertise	391
disable icmp logging.....	392
show icmp.....	392
show icmp settings.....	392
MPIP	393
delete mpip client.....	393
delete mpip server	393
Multicasting.....	394
set ip multicast heartbeat.....	394
set ip multicast proxy interface.....	394
IGMP	395
join ip igmp <IP_multicast_address>	395
leave ip igmp <IP multicast address>.....	395
list ip igmp.....	395
set ip igmp [eth:1 eth:2 slot:x/mod:y]	396
show ip igmp [eth:1 eth:2 slot:x/mod:y]	397
OSPF and Policy- Based Routing	398
add ospf cryptographic_key <key_id>.....	398
add ospf receivepolicy.....	399
add ospf sendpolicy	401
show ospf sendpolicy <IP address> source	402
delete ospf cryptographic_key	403
delete ospf default_area	403
delete ospf receivepolicy <network_address/ mask>.....	403
delete ospf sendpolicy	404
disable ospf	405
disable ospf area.....	405
disable ospf interface.....	405
enable ospf.....	406
enable ospf area	406
enable ospf interface	406
list ospf.....	407
list ospf cryptographic_key.....	407
list ospf host.....	408
list ospf interface	408
list ospf lsdb all	409
list ospf neighbor.....	409
list ospf receivepolicy	410

list ospf sendpolicy	410
set ospf area	411
set ospf cryptographic_key	412
set ospf default_area_id	413
set ospf global	413
set ospf host	414
set ospf interface	415
set ospf receivepolicy <network_address/ mask>	416
set ospf sendpolicy	418
show ospf	419
show ospf area <area_id> settings	419
show ospf cryptographic_key	420
show ospf global settings	421
show ospf interface <IP address or IF index> settings	422
show ospf interface <IP address or IF index> counters	423
show ospf lsdb	424
show ospf receivepolicy <network_address>	424
show ospf sendpolicy	425
PPP	425
add datalink ppp user <username>	425
delete datalink ppp interface	425
disable ilmi	426
disable ppp acct_for_abnormal_disc	426
disable ppp address_field_compression	426
disable ppp bacp_bap	427
disable ppp multilink_ppp	427
disable ppp offloading	427
disable ppp protocol_field_compression	428
disable ppp receive_accm	428
disable datalink ppp interface	428
enable atm1483 pvc	428
enable atm1577 pvc	429
enable atmsig	429
enable datalink ppp interface	430
enable ilmi	430
enable ppp acct_for_abnormal_disc	430
enable ppp address_field_compression	430
enable ppp bacp_bap	431
enable ppp multilink_ppp	431
enable ppp offloading	431
enable ppp receive_accm	431
enable ppp protocol_field_compression	432
enable ppp radius_challenge_with_pap	432
disable ppp radius_challenge_with_pap	432
monitor ppp	432
show ppp settings	436
enable ppp send_edo	437
disable ppp send_edo	437

PPPoE Commands.....	437
add pppoe service_name	437
delete pppoe service_name.....	438
disable pppoe on interface.....	438
enable pppoe on interface	438
show pppoe	438
list pppoe	439
list virtual connections	439
set pppoe	439
Tunneling.....	440
list all sessions vpn	440
list all tunnels.....	440
list tunnel connections.....	440
set global_call_type	441
show global_call_type settings.....	441
show pptp tunnel	441
show pptp tunnel <number> session <number>.....	443
L2TP	445
add l2tp lns <1 to 9> address <IP address>	445
delete l2tp lns.....	445
disable l2tp lcp_renegotiation_at_lns	446
disconnect l2tp tunnel	446
disconnect l2tp tunnel <number> session <number>.....	446
disable l2tp lns.....	446
enable l2tp lns	447
enable l2tp lcp_renegotiation_at_lns.....	447
list l2tp lns	447
list l2tp tunnels	448
list l2tp sessions tunnel	449
list l2tp session_counters	449
reset l2tp session_counters	449
set l2tp	450
set l2tp lns.....	451
show l2tp settings	452
show l2tp counters.....	454
show l2tp lns.....	454
show l2tp tunnel	454
show l2tp tunnel <number> session <number>.....	456
enable L2TP force_multiple_tunnels	458
disable L2TP force_multiple_tunnels.....	458
enable L2TP use_client_auth_id_for_assignment_id	458
disable L2TP use_client_auth_id_for_assignment_id	458
PPTP	459
set pptp <number>	459
add pptp pns <1-9> address <IP address>	460
show pptp settings	461
delete pptp pns	462
enable pptp pns.....	462

disable pptp pns.....	462
disconnect pptp tunnel <number>	462
disconnect pptp <number> session <number>	463
list pptp pns.....	463
list pptp tunnel <number> sessions	463
list pptp tunnels	464
Tunnel Switch.....	464
enable tunnel switch	464
disable tunnel switch.....	464
show tunnel switch_counters	465
show tunnel_switch settings	465
VTP	466
enable vtp timestamp checking	466
disable vtp timestamp checking.....	466
disconnect vtp tunnel.....	466
list vpn <0 to 65535> vtp tunnels.....	466
list vtp tunnels.....	466

7 SECURITY COMMANDS

AAA Server	467
add aaa_server.....	467
delete aaa_server	469
delete aaa_server <name> preference <number>	469
list aaa_server	469
set aaa_server	470
show aaa_server <name> preference <number>	471
Authentication Commands.....	472
disable authentication	472
enable authentication	472
set authentication	473
show authentication settings.....	475
CBCP Commands.....	477
enable ppp negotiated_callback	477
disable ppp negotiated_callback.....	477
IPsec (Policy) Commands	478
add policy	478
delete policy.....	478
IPsec (IP Security) Commands	479
enable ip security_option	479
show ip security settings	480
show security_option	480
disable ip security option.....	481
Microsoft Point to Point Encryption Commands.....	482
Network Address Translation Commands.....	482
list nat sessions	482
list nat stats.....	482
Packet Filtering Commands	483

add filter.....	483
delete filter.....	484
list filters.....	484
set interface.....	485
set packet_logging.....	486
show filter.....	487
verify filter.....	488
set policy update.....	488
RADIUS.....	489
set accounting.....	489
set accounting_backup primary.....	492
set accounting_backup secondary.....	494
set accounting_call_detail_record [disabled enabled].....	496
set accounting_server_group [a b] retransmissions.....	498
set acct_format [all simple sprint].....	498
set radius.....	499
set security_service.....	502
set service_loss_busyout radius frequency.....	502
Accounting Server Commands.....	502
disable_primary_accounting_server.....	502
enable_primary_accounting_server.....	503
enable_prioritize_first_accounting_server_in_a_group.....	503
enable_secondary_accounting_server.....	503
disable_prioritize_first_accounting_server_in_a_group.....	504
disable_secondary_accounting_server.....	504
show_accounting.....	504
show_contact.....	506
show_contact_timers.....	506
show_radius.....	506
show_radius_resource_management_settings.....	506
show_radius_resource_management_counters.....	507
show_service_loss_busyout_settings.....	507
disable_accounting.....	507
disable_accounting_server_group.....	508
disable_radius_accounting.....	508
disable_radius_fill_null_attributes.....	509
disable_radius_interim_accounting_interval.....	509
disable_radius_resource_management.....	509
disable_radius_send_acct_for_default_user.....	510
disable_radius_source_port_authentication.....	510
disable_radius_use_radius_username.....	510
disable_service_loss_busyout [ping radius].....	511
enable_accounting.....	511
enable_accounting_server_group [a b].....	511
enable_radius_accounting.....	512
enable_radius_authentication_syslog_counters.....	512
enable_radius_ignore_source_port.....	513
disable_radius_ignore_source_port.....	513

enable radius send_unauth_acct_record	513
disable radius send_unauth_acct_record	514
enable radius fill_null_attributes	514
enable radius interim_accounting_interval	514
enable radius resource_management	515
enable radius resource_free_tunnel_initiator	515
disable radius resource_free_tunnel_initiator	515
enable radius send_acct_for_default_user	516
enable radius source_port_authentication	516
enable radius use_radius_username	516
enable radius auth_fail_traps	517
disable radius auth_fail_traps	517
enable service_loss_busyout [ping radius]	517
monitor radius	518
set pbus reported_port_density	523
set pbus reported_base	523
set pbus trap	523
Security Association	524
delete sa	524
list sa	524
show sa	525
TACACS+	525
set tacacsplus interim_accounting_interval	525
show authorization settings	526
show direct_request	526
show tacacsplus settings	526
disable authorization	527
disable direct_request	527
disable tacacsplus interim_accounting_interval	527
enable authorization	528
enable direct_request	528
enable tacacsplus interim_accounting_interval	528
set direct_request timeout	529
add cleartcp encryption_ids	529
delete cleartcp encryption_ids	529
list cleartcp encryption_ids	530

8 SIGNALING SYSTEM 7 COMMANDS

SS7 Functionality	531
show system settings	531
SS7 Commands	532
connect ss7 gateway	532
connect ss7 slot <slot_list>	532
disable ss7 slap_down_trap	532
disable ss7 slap_up_trap	532
disable ss7 slot_down_trap	533
disable ss7 slot_up_trap	533

disable ss7 trace	533
disconnect ss7 gateway	533
disconnect ss7 slot.....	533
enable ss7 slap_down_trap.....	534
enable ss7 slap_up_trap.....	534
enable ss7 slot_down_trap	534
enable ss7 slot_up_trap	534
enable ss7 trace.....	534
list ss7 slots.....	535
reset ss7 counters	535
send ss7 heartbeat.....	535
set ss7 protocol [slap_v2]	536
set ss7 slot.....	537
set ss7	537
show ss7	538
show ss7 counters	538
show ss7 slap status	538
show ss7 slot <slot_list> counters	539
show ss7 trap status	539

ALPHABETICAL COMMAND LISTING

INDEX

LIST OF TABLES

Table 1	Notice Icon Descriptions.....	xxxiii
Table 2	Text Convention Descriptions.....	xxxiv
Table 3	IP Network Address Syntax	44
Table 4	Case-sensitive Examples.....	44
Table 5	Command Line Edit Commands.....	51
Table 6	Command History Retrieval Commands	52
Table 7	Set Date and Time Parameters	55
Table 8	Set Command Parameter Descriptions	64
Table 9	Set System Command Parameter Descriptions	65
Table 10	Set Bootrom Command Parameter Descriptions.....	68
Table 11	Set Bootrom IP Interface Command Parameter Descriptions.....	68
Table 12	Add Syslog Command Parameter Descriptions	72
Table 13	Set Syslog Command Parameter Descriptions.....	76
Table 14	Show Syslog Fields and Descriptions	77
Table 15	Show Syslog Fields and Descriptions	80
Table 16	Show Bootrom Settings Display Information	87
Table 17	Show Command Settings Display Information.....	88
Table 18	Show Statistics Command Parameter Descriptions	94
Table 19	Reset Command Parameter Descriptions.....	95
Table 20	Reset Statistics Command Parameter Descriptions.....	96
Table 21	Send Command Parameter Descriptions	143
Table 22	Enable Telnet Command Parameter Descriptions	145
Table 23	Disable Telnet Command Parameter Descriptions.....	146
Table 24	Add User Command Parameter Descriptions.....	147
Table 25	Set User Command Parameter Descriptions	151
Table 26	Set Dialout User Command Parameter Descriptions	154
Table 27	Set Dialout User site Command Parameter Descriptions	155
Table 28	Set Framed_Route User Command Parameter Descriptions	156
Table 29	Set Login User Command Parameter Descriptions	157
Table 30	Set Network User Command Parameter Descriptions	158
Table 31	Set Network User Command Parameter Descriptions	159
Table 32	Set Network Command Parameter Descriptions	160
Table 33	Set Network User Command Parameter Descriptions	162
Table 34	Set Network User PPP Command Parameter Descriptions.....	164
Table 35	Set Tunnel User Command Parameter Descriptions	166
Table 36	Set DHCP_Proxy Command Parameter Description.....	173
Table 37	Show DHCP_Proxy Settings.....	174
Table 38	List DHCP_Proxy Leases.....	174
Table 39	Show DHCP_Proxy Counters.....	175
Table 40	Add Login_Host Parameter Descriptions.....	175
Table 41	Add Login_table Parameter Description	177
Table 42	List Login Hosts Description	179
Table 43	Rlogin Command Description	181
Table 44	Set Login_host Preference Description	182
Table 45	Set Login_table Command Parameter Descriptions	183
Table 46	Add Ping Service_Loss_System Command Parameter Descriptions.....	184
Table 47	List Ping Service_loss_systems Description	185
Table 48	List Ping Display Information	186
Table 49	Ping Parameter Description	187
Table 50	Set Ping Service_Loss_System Command Parameter Descriptions	189
Table 51	Show Ping Server Settings Description	190
Table 52	Add SNMP community Command Parameter Descriptions	193
Table 53	Add SNMP Community_pool Parameter Descriptions.....	193

Table 54	Add SNMP Trap_Community Command Parameter Descriptions	194
Table 55	Add SNMP Trap Community Pool Command Parameter Descriptions	195
Table 56	Delete SNMP Community_Pool Command Parameter Descriptions	196
Table 57	Delete SNMP Trap Community Pool Parameter Descriptions	196
Table 58	List SNMP Communities Description	199
Table 59	List SNMP Trap_communities Description	200
Table 60	Set SNMP Community Command Parameter Descriptions	201
Table 61	Set SNMP Trap_Community Command Parameter Descriptions	202
Table 62	Add TFTP Request Command Parameters Descriptions	204
Table 63	Set TFTP Request Command Parameter Descriptions	207
Table 64	TFTP Command Descriptions	207
Table 65	Add IP Pool Command Parameter Descriptions	210
Table 66	Add MPIP Client Command Parameter Descriptions	211
Table 67	Add MPIP Server Command Parameter Descriptions	212
Table 68	List MPIP Links Description	213
Table 69	Set Connection Command Parameter Descriptions	215
Table 70	Set IP Pool Command Parameter Descriptions	216
Table 71	Set IPX System Command Parameter Descriptions	218
Table 72	Set PPP Command Parameter Descriptions	220
Table 73	Set MPIP Command Parameter Descriptions	221
Table 74	Set MPIP Client Command Parameter Descriptions	222
Table 75	Set MPIP Server Command Parameter Descriptions	222
Table 76	Set NTP Command Parameter Descriptions	224
Table 77	Add Modem_Group Command Parameter Descriptions	228
Table 78	Assign Interfaces Command Parameter Descriptions	228
Table 79	Add Network Service Command Parameter Descriptions	231
Table 80	Data Parameter Descriptions	232
Table 81	Set Network Service Command Parameter Descriptions	235
Table 82	List Interface Description	247
Table 83	List IP Interface_block Description	247
Table 84	List Switched Interface Description	248
Table 85	Set DS1 Interface Command Parameters Descriptions	249
Table 86	Set Logical DS1 Interface Command Parameters Descriptions	251
Table 87	Set Switched Interface Parameter Descriptions	253
Table 88	Set Sync Interface Command Parameter Descriptions	259
Table 89	Set Chassis Slot Command Parameters Descriptions	271
Table 90	Add Init_Script Command Parameters Descriptions	273
Table 91	Set INIT_Script Command Parameters Descriptions	275
Table 92	Set Modem_Group Command Parameters Descriptions	278
Table 93	Add Tap Interface Command Parameters Descriptions	292
Table 94	Add Tap Next Command Parameters Descriptions	293
Table 95	Add Tap User Command Parameters	294
Table 96	Set Tap ID Command Parameters	296
Table 97	Set Tap User Command Parameter	297
Table 98	Add ATM_ARP_Server Parameter Description	300
Table 99	Add IP ARP Address Command Parameters Descriptions	300
Table 100	Add IP ARP Address Command Parameters	301
Table 101	Delete IP ARP Address Command Parameters	302
Table 102	List IP ARP Description	304
Table 103	Show IP INVARP Parameter Description	305
Table 104	List IP INVARP Network Description	306
Table 105	Add ATM1483 PVC Command Parameters Descriptions	307
Table 106	Add ATM 1577 PVC Command Parameters Descriptions	308
Table 107	Set ATM Options Command Parameters Descriptions	311
Table 108	Set ATM_Address Network Command Parameters Descriptions	312
Table 109	Show ATMCFG Parameter Descriptions	313



Table 110 Add IP Defaultroute Gateway Command Parameters Descriptions.....	314
Table 111 Add IP Network Command Parameters Descriptions	315
Table 112 Add IP Route Command Parameters Descriptions.....	316
Table 113 Add Framed_Route User Command Parameters Descriptions	317
Table 114 Add IP Source Route Command Parameters Descriptions	318
Table 115 Add IPX Network Command Parameters Descriptions	318
Table 116 Add IPX Route Command Parameters Descriptions	319
Table 117 Add IPX Service Command Parameters Descriptions.....	320
Table 118 IPX Service Types and Descriptions.....	321
Table 119 Delete IPX Service Command Parameters Descriptions	325
Table 120 Disable IP Command Parameters Descriptions	326
Table 121 Enable IP Command Parameters Descriptions.....	333
Table 122 Set IP ARP Address Command Parameters Descriptions.....	347
Table 123 Set IP Default Router Command Parameters Descriptions.....	348
Table 124 Set IP Network Command Parameters Descriptions.....	350
Table 125 Set IP Router Command Parameters Descriptions.....	351
Table 126 Set IP Routing Command Parameters Descriptions	352
Table 127 Set IP Source Based Routing Command Parameters Descriptions.....	353
Table 128 Set IP Source Route Command Parameters Descriptions.....	353
Table 129 Set IPX Network Command Parameters Descriptions.....	355
Table 130 Add Cross_Connect Command Parameters Descriptions.....	363
Table 131 Set Add DNS Host Command Parameters Descriptions.....	365
Table 132 Add DNS Server Command Parameters Descriptions	366
Table 133 Set DNS Command Parameters Descriptions	372
Table 134 Set DNS Server Preference Command Parameters Descriptions.....	373
Table 135 Set Frame_Relay Interface Parameters Descriptions	383
Table 136 Set Frame_Relay PVC Command Parameters Descriptions	385
Table 137 Set IP Multicast Heartbeat Command Parameters Descriptions	394
Table 138 Set IP IGMP Command Parameters Descriptions.....	396
Table 139 Add OSPF Cryptographic Key Command Parameters Descriptions.....	398
Table 140 Add OSPF Receivpolicy Command Parameters Descriptions	400
Table 141 Add OSFP Command Parameters Descriptions	401
Table 142 Delete OSPF Command Parameters Descriptions.....	404
Table 143 Delete OSPF Command Parameters Descriptions.....	404
Table 144 List OSPF Command Parameters Descriptions.....	407
Table 145 Set OSPF Command Parameters Descriptions.....	411
Table 146 Set OSPF Command Parameters Descriptions.....	412
Table 147 Set OSPF Global Command Parameters Descriptions	414
Table 148 Set OSPF Interface Command Parameters Descriptions.....	415
Table 149 Set OSPF Receiving Command Parameters Descriptions.....	417
Table 150 Set OSPF SendPolicy Command Parameters Descriptions.....	418
Table 151 Show OSPF Command Parameters Descriptions	419
Table 152 Add Datalink PPP User Command Parameters Descriptions	425
Table 153 List PPPOE Command Parameters Descriptions.....	439
Table 154 Set PPPOE Command Parameters Descriptions.....	440
Table 155 Set L2TP Command Parameters Descriptions.....	450
Table 156 Set 12TP LNS Command Parameters Descriptions	452
Table 157 Set PPTP Command Parameters Descriptions.....	459
Table 158 Add AAA_Server Command Parameters Descriptions.....	468
Table 159 Set AAA_Server Command Parameters Descriptions	470
Table 160 Show AAA_Server Parameter Descriptions	471
Table 161 Disable Authentication Parameters Descriptions.....	472
Table 162 Enable Authentication Parameters	473
Table 163 Set Authentication Command Parameters Descriptions.....	474
Table 164 Add Policy Command Parameters Descriptions.....	478
Table 165 List Filter Command Description.....	484

Table 166 Set Interface Parameter Description	485
Table 167 Set Packet_Logging Command Parameter Descriptions	486
Table 168 Set Accounting Parameter Commands	490
Table 169 Set Accounting Backup Primary Commands	493
Table 170 Set Accounting Backup Secondary Commands	495
Table 171 Set Acct_format Descriptions	498
Table 172 Set RADIUS Command Parameters Descriptions	500
Table 173 Disable Radius Accounting Command Parameters	508
Table 174 Enable Radius Accounting Command Parameters Descriptions	512
Table 175 Set Pbus Trap Command Parameters	524
Table 176 Disable SS7 Trace Command Parameters	533
Table 177 Enable SS7 Trace Command Parameters	534
Table 178 Set SS7 Protocol Slap_v2 Command Parameters	536
Table 179 Set SS7 Command Parameters Descriptions	537

ABOUT THIS GUIDE

About This Guide includes an overview of this guide, lists guide conventions, related documentation, and product compatibility, and provides contacting CommWorks information.

This guide describes the various components of the CommWorks Total Control® 1000 Enhanced Data System and how they work together to build a communications platform for integrating local and wide area networks.

This guide is intended for network administrators or engineers who will be installing and configuring the Total Control 1000 system for use with their applications.



Release notes are issued with some products—visit our website at <http://totalservice.commworks.com>. If the information in the release notes differs from the information in this guide, follow the instructions in the release notes.

Conventions

[Table 1](#) lists notice icons used in this guide:

Table 1 Notice Icon Descriptions

Icon	Notice Type	Description
	Information Note	Information that contains important features or instructions.
	Caution	Information to alert you to potential damage to a program, system, or device.
	Warning	Information to alert you to potential personal injury or fatality. May also alert you to potential electrical hazard.
	ESD	Information to alert you to take proper grounding precautions before handling a product.

[Table 2](#) lists text conventions in this guide.

Table 2 Text Convention Descriptions

Convention	Description
Text represented as a screen display	This typeface represents displays that appear on your terminal screen, for example: Netlogin:
Text represented as menu or sub-menu names .	This typeface represents all menu and sub-menu names within procedures, for example: On the File menu, click New .
Text represented by <filename>	This typeface represents a variable. For example: <filename>.

Related Documentation

The following documents contain additional information about Total Control 1000 components, operations, systems, and procedures that may be referenced in this manual:

Total Control 1000 Enhanced Data System

The following documents relate to the Total Control 1000 Enhanced Data System:

- Total Control 1000 Enhanced Data System *System Overview Guide* - Part Number 10048404
- Total Control 1000 Enhanced Data System *Getting Started Guide* - Part Number 10048403
- Total Control 1000 Enhanced Data System *Operations Guide* - Part Number 10048402
- Total Control 1000 Enhanced Data System *Maintenance Guide* - Part Number 10048391
- Total Control 1000 Enhanced Data System *Trouble Locating and Clearing Guide* - Part Number 10048400
- Total Control 1000 Enhanced Data System *DSP Multispan Command Line Reference* - Part Number 10048399
- Total Control 1000 Enhanced Data System *Access Router Card 5.5 Command Line Reference* - Part Number 10048398
- CommWorks 5115 Common Element Manager *User's Guide* - Part Number 10047652
- CommWorks 5115 Common Element Manager for Total Control 1000 *User Guide* - Part Number 10048397

Total Control HiPer System

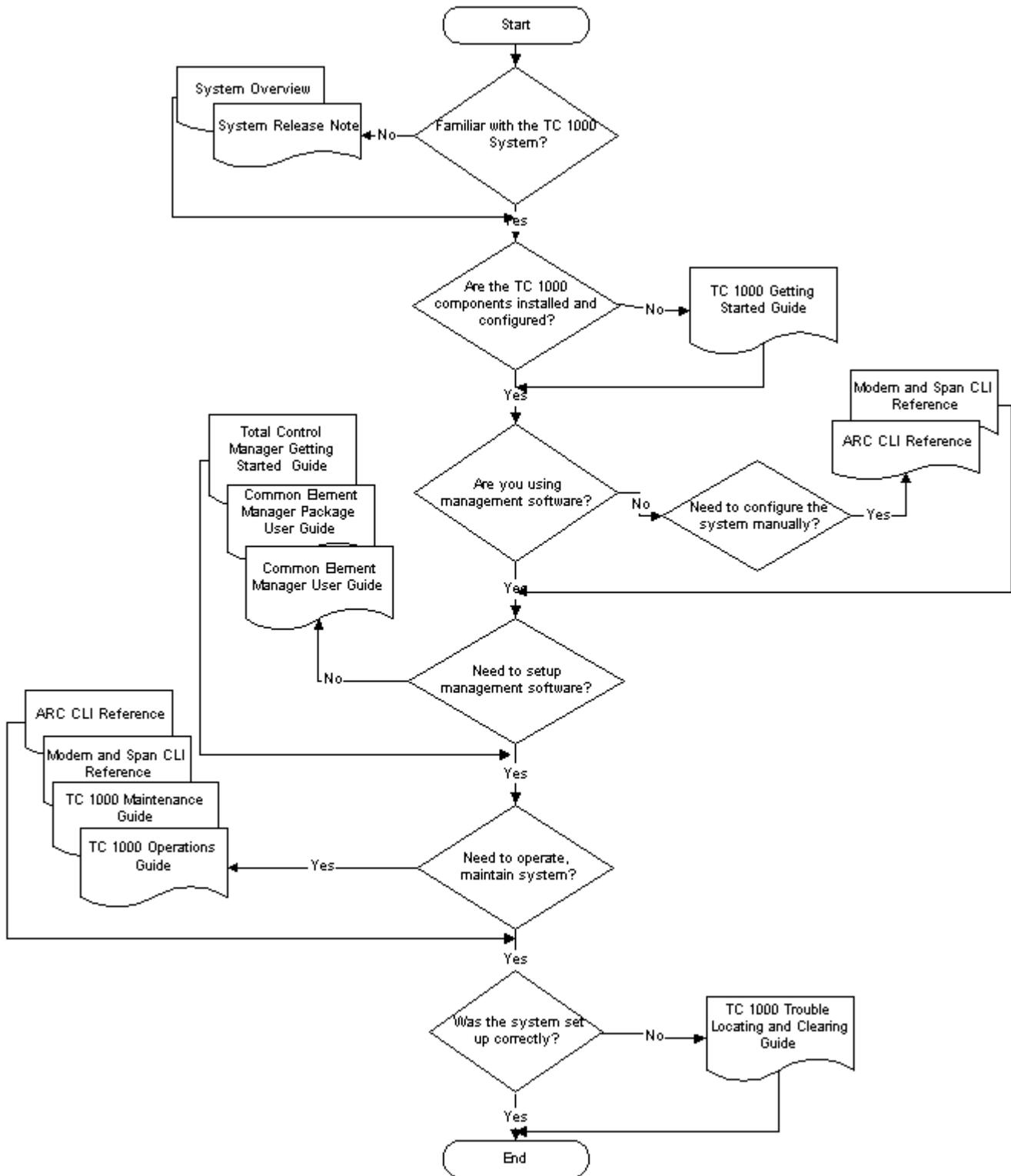
Some documents from the Total Control MultiService Access Platform (the HiPer system) also relate to the Total Control 1000 Enhanced Data System.

- HiPer ARC Network Application Card *Getting Started Guide* - Part Number 10031739

- PCI Dual 10/100Base-T Ethernet Network Interface Card *Getting Started Guide* - Part Number 1.024.1330-02
- PCI Dual V.35 10/100 Ethernet PCI Network Interface Card *Getting Started Guide* - Part Number 1.024.1959-01
- Quad T1/E1 10/100 Ethernet PCI Network Interface Card *Getting Started Guide* - Part Number 1.024.1973-00
- Dual DS3 Asynchronous Transfer Mode Network Interface Card *Getting Started Guide* - Part Number 10030485
- Dual E3 Asynchronous Transfer Mode Network Interface Card *Getting Started Guide* - Part Number 10031642
- HiPer DSP Network Application Card *Getting Started Guide* - Part Number 10030920
- HiPer DSP T1/E1 Network Interface Card *Getting Started Guide* - Part Number 1.024.1310-02
- HiPer NMC Network Application Card *Getting Started Guide* - Part Number 10030486
- 10/100 Ethernet Aux I/O Network Application Card *Getting Started Guide* - Part Number 1.024.1309-01

Use the following documentation map to help you install and configure your Total Control 1000 system.

Figure 1 Documentation Map



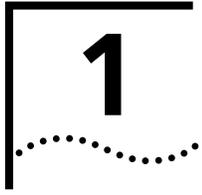
Contacting Customer Service

For information about Customer Service, including support, training, code releases and updates, contracts, and documentation, visit our website at <http://totalservice.commworks.com>.

Refer to the Documentation CD-ROM for information about product warranty.

Before contacting Technical Support, have this information available:

- Contract number
- Problem description
 - Symptoms
 - Known causes
- Product information
 - Software and hardware versions
 - Serial numbers
- Trouble locating and clearing attempts



USING THE COMMAND LINE INTERFACE

This chapter describes some basic concepts of the Command Line Interface (CLI) including the syntax and structure of the command language.

The chapter contains the following sections:

- [Overview](#)
- [Accessing the Command Line Interface](#)
- [Command Format](#)
- [Entering Commands](#)
- [Command Language Structure](#)
- [Command Line Interface Conventions](#)

Overview

The CLI is the user interface used to communicate with the access router card, using text-based input and output.

The CLI allows you to add, remove, and modify configurations, start and stop services, and directly or remotely manage and monitor the access router card.

Accessing the Command Line Interface

CLI commands are entered after establishing a connection with the access router card. A connection must be made to the card to access the CLI. This is done using:

- a direct null-modem connection
- a Telnet session once the card has an IP address

Command Format

Many commands are multi-tiered, position-independent, and use keywords. With multi-tiered commands, you type the base command, such as:

```
set interface
```

followed by parameters specific to that base command, such as:

```
host_type
host_address
```

Position-independent commands do not require all parameters to be specified at once, nor in sequence, to work. Entering a *keyword* in the base command such as `network` in **add ip network** is mandatory to enable the command.

Command syntax is described in the example below:

```
add ip network <network name> address [IP address]
    {enabled [no | yes] }
    {frame [ethernet_II, snap] }
    {interface [eth:1 or eth:2] }
```

add ip network is the base command

<network name> and **address [IP address]** are required values.



Required parameters are included under the Syntax heading. If available, an example follows showing a valid entry.

{enabled [no | yes] } is the network “on” value with options.

{frame [ethernet II, snap] } is the encapsulation type with options.

{interface [eth:1 or eth:2] } is the LAN connection with options.

Parameters

Braces, arrows, and brackets explain parameter listings and the required or optional values.

- **{ ... }** parameters enclosed in *braces* are optional and are provided with *default* values. You do not need to specify these parameters unless you wish to override the default.
- **< ... >** values enclosed in *arrows* are used by a command or parameter which is position-dependent and does not have keywords. Some of these parameters are required and some are not. Required values are displayed in the CLI when querying a command (typing a question mark) or upon issuing a command where required values were omitted.
- **[...]** range of values following keywords are enclosed in *brackets*. Inside brackets, the vertical bar (pipe) and comma separate values.

- | (pipe or vertical bar)—you may select only *one* from the *key list*: [first | second | third]
- , (comma)—you can select *one or more* of the displayed *bitmasks*: [first, second, third,...]
- *Position independent* arguments are shown in a vertical array after the command.

Syntax, Examples, and Related Commands

Each command is structured with the syntax, examples, and related commands.

The syntax shows the complete nomenclature of the command, with required and optional parameters.

Examples provide a sample of what is entered, filling in actual values for required and optional parameters. Note that many of the examples containing system-specific information (IP addresses, subnet masks, etc.) will not work on every system. With other commands, the example is the same as the syntax (`show all`).

Related commands direct you to commands used in conjunction with the current listing.



Example and Related Command sections are listed when available and may not be present for every command.

Entering Commands

The CLI allows you to enter commands in abbreviated form if the portion of the command you type is unique—refer to [Abbreviation and Command Completion](#) for more information. You can also use command completion and positional help when entering command strings.

Using Control Characters

Control characters provide increased functionality when working with CLI, such as recalling previous commands, positioning text and cursors, and stopping processes.

- While working in the CLI, system messages may scroll across your screen. Use **Ctrl L** to retrieve the last command entered. This is helpful if you are unsure exactly where you were when you received the system message.
- If you have typed ahead to enter a series of commands, and you want to stop processing your commands, press **Ctrl C** to abort any currently executing and stacked commands.
- Retrieve commands by typing **Ctrl P** for previous and **Ctrl N** for next. Command retrieval consults the history of previous fully entered commands, defaulting at the last ten commands. If an error occurs while a command is processing, any partial command (up to and including the field in error) is added to the history list.
- Command line editing allows these options:

- **Ctrl B** or *left arrow* brings you go back one character
- **Ctrl C** deletes the running CLI process
- **Ctrl F** or *right arrow* takes you forward one character
- **ESC B** takes you back one word
- **ESC F** takes you forward one word
- **Ctrl A** takes you to the beginning of a command
- **Ctrl E** takes you to the end of a command
- **Ctrl D** or **Ctrl K** deletes a selected character

Abbreviation and Command Completion

You can abbreviate commands if the arguments are unique. For example, enter:

```
se us jay pa bird
```

as an acceptable abbreviation for:

```
set user jay password bird
```

However, the abbreviation:

```
se us jay m bird
```

is not an acceptable abbreviation because it is not unique — `m` can stand for `message` OR `modem_group`.



*Identifiers such as **password** in the above example are not completed. For brevity, some commands in this chapter are abbreviated and annotated (abbr.).*

Some parameters are omitted in examples because they default to standard values and do not require entry, or are unnecessary for common configuration.

Command completion finishes spelling a unique, abbreviated value for you just by pressing the TAB key. This is handy as a time-saving device or when uncertain about a command.

For example, if you type `add ip n` and press the TAB key, it will spell out the keyword `network` without losing your place in the command syntax.

Help Help is *general* or *positional*. Enter:

```
help <any command keyword>
```

to get a cursory list of commands and syntax. Enter

```
<any command> ?
```

to get more extensive, positional help for a particular field. Help is most useful during configuration: query the list of possible parameters by typing `?` and, when you find the appropriate value, type it without losing your place in the argument. Be sure to leave a space between the keyword and the question mark.

Additional Conventions

The type of value you enter must match the type requested. Numbers are either decimal or hexadecimal. Text can be either a string that you create, or it may be a list of options you must choose from. When choosing an option, type the text of the option exactly.

- “Double quotation marks” set off user-defined *strings*. If you want white space or special characters in a string, it must be enclosed by “double quotation marks.”
- If a keyword is not *unique*, it will “ding.” Then, if you wish to list possible keywords, you may use positional help.
- Most commands are *not* case sensitive. As a rule, only *<name>* and *[password]* values require typing the correct case.
- Configuration changes are lost upon reboot unless you save them. Use the `save all` command to save configuration changes permanently in Flash memory. Changes are also lost by the access router card if power fails before they are saved.
- Some commands such as `add ip network` and `reconfigure` do **not** take effect immediately.
- Some `delete` commands require that you first *disable* the process or function. For example, commands to delete a network user, interface, and network service must first be disabled.
- In most cases, wherever an *IP address* value is required, you can enter a host *name*, provided you have configured a DNS server or put the name and address into the DNS Local Host Table.
- You can create a script file (a text file containing CLI commands) to simplify repetitive tasks. Use TFTP to transfer the file to the Flash file system, then use the `do` command to run the script file.

Network Address Formats

Many commands require a network address to define a link to a remote host, workstation or network. IP and IPX network addresses shown in this document use the syntax described in the following table. IP netmasks are configured three ways:

- Using the CLI mask signifier (A,B,C or H)
- Using the standard format (xxx.xxx.xxx.xxx)
- Counting the one bits in a range from 8 to 30 (32 for a host)

[Table 3](#) lists information about IP network address syntax.

Table 3 IP Network Address Syntax

Address Type	Format	Range
IP_address	a.b.c.d	<ul style="list-style-type: none"> ■ 0.0.0.0 to 255.255.255.255 (decimal). ■ address 127.x.x.x is reserved for Loopback. ■ address 247.x.x.x or higher is not part of a valid IP Network Class (A, B, C) ■ address 0.0.0.0 is invalid in most contexts.
ip_net_address	a.b.c.d/mask	255.255.255.255/A,B,C,H or xxx.xxx.xxx.xxx or 8 to 30 bits
ipx_net_address	xxxxxxx	hexadecimal
mac_address	xx:xx:xx:xx:xx:xx	hexadecimal digit pairs
ipx_hostaddress	xxxxxxx.xx:xx:xx:xx:xx:xx	IPX network address.MAC (Ethernet) address

Interface Ranges

Interfaces can be expressed as variants of the **slot:x/mod:y** format where *x* is the slot number of the Total Control Hub and *y* is a modem number (port) from 1 to *y* depending on the type of modem card installed on the Hub. You can specify more than one interface or a range a couple ways. For example:

```
assign interface slot:4/mod:[1-3]
assign interface slot:4/mod:[1-3],slot:6/mod:15,slot:8/mod:[9-11]
```



You cannot set interfaces using ranges. The `set interface` and `set switched interface` commands require modem-by-modem configuration.

Names

You can specify names for networks, users, and other system entities. Most names can be up to 64 ASCII characters, unless specified otherwise in the command description. A name can contain white space or other non-alphanumeric characters if you enclose the name with double quotes. Note that names are case-sensitive.

[Table 4](#) shows case-sensitive examples.

Table 4 Case-sensitive Examples

Desired name:	Entered as:
Mary's PC	"Mary's PC"
Server_number_3	Server_number_3

Interface Names

Interface names follow the same rules as other names as described above, but are limited to a maximum size of 32 ASCII characters. Use the `list interfaces` command to see a list of the assigned interfaces.

Users A *user entity* is a table of parameters used when establishing a network connection. The `add user` and `set user` commands define the parameters of a user. The user commands are employed when making WAN network (dial-in) connections and for dial-out users. Local users (stored in the User Table) are limited to 450 entries.

Default User The *default user* is a powerful and efficient tool created at system setup. Designed to be applied as a template for multiple-user configuration, you can use it to change many parameters of users you subsequently configure.

For example, if you want to configure *all* your users to be *type callback*, enter:

```
set user default type callback
```

The parameters that can be configured across the board are indicated by a (D) when you type `show user <name>`. Be aware that when you use this tool, you change the *default user* factory settings.

To view the default user settings on your system enter:

```
show user default
```

Remember that to make configuration changes on an *individual* user basis, you must use the appropriate `set` commands.

Command Language Structure

The CLI command language creates, manages, displays, and removes system entities that describe system and network connections and processes. Configured entities are stored in tables such as the IP Routing Table.

Some common entities are:

- **Network**—defines local and remote networks, network connections, hosts and routers.
- **User**—describes connection parameters, for operation and authorization.
- **Modem Group**—specifies switched interfaces to be managed as a group.
- **Filter**—can be applied to interfaces, connections, and users to control access through the system.
- **Interface**—describes physical devices (e.g. ports).
- **Syslog Host**—receives system messages.
- **DNS Server**—translates IP addresses to and from host names.
- **Login Host**—made available for user connections.
- **Route**—describes a path through the network to another system/network.

Table entries are created with the `ADD` command, and removed with a `DELETE` command. The `ADD` command specifies the most important parameters of the entry. Additional parameters are usually specified with the `SET` command, which is also used to change configured parameters.

LIST commands display table entries. For example, to display all defined modem groups, enter:

```
list modem_groups
```

SHOW commands display detailed information about a specific table entry or a set of scalars (non-table items). For example, to display information on the CommWorks modem group enter:

```
show modem_group Commworks
```

The `show all` commands display information. The `show all` commands display all parameters for *all entries* in tables associated with particular commands.

The order of items in a table is usually not relevant, nor is it inherent in the type of entity. Sometimes the order is relevant, though, and you must specify a *preference* value in the ADD command, indicating where this item belongs in the table. For example:

```
add dns server <server_name> preference 1
```

This command assigns a priority of 1 to this DNS server. The DNS server with the highest preference number will be used first. Login hosts also require a preference number.

Command Line Interface Conventions

This section provides general information about CLI command conventions and usage.

Most commands are not case sensitive.

You can type most commands and parameters in upper or lower case except for the *<name>* value which requires typing the correct case. The `kill <process name>` command *is* case sensitive.

Many commands are position-independent, multi-tiered, and have keywords.

Multi-tiered commands let you type the base command (e.g. `set interface`) and implement associated parameters (*filter_access*, *input_filter*, etc.). Position-independence does not require all parameters to be specified at once, nor in sequence, to work. But typing a keyword in the base command such as `network` in `set ip network` is mandatory to enable the command.

You can abbreviate commands.

Shorten most commands and command options by typing the first few letters that distinguish that command from any other. For example, while the full command is `list tcp connections`, enter `li tc` to invoke it.



An error message displays if you type an ambiguous abbreviated command.

Double quotations distinguish text strings.

Add white space or special characters to a string by wrapping it in double quotes.

Command syntax and CLI rules.

This document uses the following CLI command syntax conventions:

- The base command is listed in the left margin.
- The full syntax of the command with parameters (required and optional) is listed in the **Syntax** section.
- Values that are position dependent and do not have keywords are in *carets*. For example: `<ip_address>`. Some of these parameters are required and some are not. Required values are displayed in the CLI when querying a command (typing a question mark) or upon issuing a command where required values were omitted.
- *Position independent* arguments display vertically after the command. For example:

```
set dns
    domain_name <name>
    number_retries <1 to 5>
    timeout <5 to 125 seconds>
```

- A *vertical* character between parameters indicates a choice of options. For example:

```
<yes|no>
```

- *Commas* between a series of choices indicates multiple options. For example:

```
[login, network, callback, dial_out, manage, location]
```

Command completion

Finish spelling a unique, abbreviated command parameter by pressing the **TAB** key. It is helpful to speed up input or verify a command value.

For example, if you type `add ip n` and press **TAB**, command completion spells out the keyword **network** without losing your place in the command syntax. If the keyword is *not* unique, the CLI will not auto-complete.

Command retrieval

Recall an earlier command by pressing **Ctrl P** or advance to the next command by pressing **Ctrl N**. Command retrieval consults the history of previous commands entered, defaulting to the last 10 commands. To change the depth of the buffer holding command history enter:

```
set command history
```

To view current depth and a list of your last issued CLI commands enter:

```
history
```

Command reprint

Press **Ctrl L** to re-display what you typed before pressing the **ENTER** key.

Command Line Editing

Command line editing offers these options:

- **Ctrl b** or left arrow retreats one character
- **Ctrl c** closes a CLI process
- **Ctrl f** or right arrow advances one character
- **ESC b** retreats one word
- **Esc f** advances one word
- **Ctrl a** advances to the beginning of a command
- **Ctrl e** retreats to the end of a command
- **Ctrl d** or **Ctrl k** deletes the selected character.

Paused (--More--) output display

When the access router card outputs more information than your screen can accommodate, you can invoke a “more” pager for one more line or page of output or cancel the request. It works as follows. At the point on your screen where output breaks (-- More --), pressing:

- **ENTER** or **Ctrl m**—produces one more line of output
- **ESC**—produces one more page of output
- **q** or **Ctrl c**—cancels the output request

Two commands enable page breaks for commands which display long text output: `list`, `show`, et al. One command runs globally (for all access router card sessions) and the other locally (for the current session) They are:

```
enable command global_terminal_settings_page_breaks
enable command local_terminal_settings_page_breaks
```

The following command varies the number of rows output to your screen:

```
set command global_terminal_settings_rows <1 to 256>
```

Using general and positional help

The access router card includes general and positional help to assist you in determining the proper command syntax.

For *general* help, enter:

```
help <any command>
```

A cursory list of associated commands and their proper syntax is provided.

Positional help is available when entering a command by typing a question mark (?) after the command. The CLI displays possible completions and returns the cursor to the point in the command before you entered the question mark.

First disable, then delete objects

Some *delete* commands require that you first *disable* the object or function. Deleting an IP network, for instance, first requires that you *disable* it. But if you issue the `reconfigure ip network` command, the access router card automatically reconfigures network parameters of any established static IP LAN network. This command changes network parameters without you having to remove the router from service.

Saving changes

Save changes using the `save all` command. It is important to remember that most commands may be accepted when entered, but not necessarily *saved* across reboots until you use the `save all` command.

Running and stopping processes

The access router card encompasses many standard processes which are transparent to the user. Administrators can run them issuing the `do` command, or end them using the `kill <process name>` command. This is useful for diagnostic or test purposes. Refer to [Chapter 2, "Management Commands,"](#) for more information.

Using network services

The following network services are provided:

- *ClearTCPD*—a daemon enabling ClearTCP access to a modem group.

- *SNMPD*—an SNMP agent utilizing the UDP protocol.
- *TELNETD*—a TELNET daemon to access either the CLI or a modem group.
- *TFTPD*—a TFTP daemon utilizing UDP on the server side of the network to access files.
- *RSHD*—a daemon supporting RSH and RCP using TCP.

Using add and set commands

Issue `add` and `set` commands to set and change system parameters. These matched commands are functionally related, but also differ dramatically. Table entries such as `user`, `interface`, `network`, etc., require the `add` command to set initial parameters. Then use the `set` command to edit those parameters.

Using list and show commands

Issue `list` and `show` commands to view table entries or a detailed table entry. The `list` command displays a list of table entries only, while the `show` command displays information about *a single line in a table* or a set of *scalars* (non-table items). The `show all` commands display all parameters for *all entries* in tables associated with particular commands.

Rebooting

In general, rebooting is rarely required but changing settings on the fly can sometimes cause inconsistent behavior in the access router card. Therefore, if you edit your configuration and want to ensure the changes are accepted, save your work using the `save all` command and issue the `reboot` command. A more flexible, feature-rich alternative employs the *Boot Configuration* menu to retrieve a configuration from Flash memory or a network source as well as provides a host of other options.

2

MANAGEMENT COMMANDS

This chapter provides information about command features and describes the following types of management commands:

- [Administrative Commands](#)
- [CLI Exit Commands](#)
- [EEPROM](#)
- [Event Logging Commands](#)
- [IP Network Commands](#)
- [Show All Commands](#)
- [Statistics](#)
- [Telnet Commands](#)
- [Telnet Commands \(Console Port\)](#)
- [TCP](#)
- [User Commands](#)

Command Features

The command language has several built-in features that make it easier to use. When abbreviating commands, it is sometimes difficult to remember commands and their syntax. Use [Positional Help](#) and [Command Completion](#) to refresh your memory of the commands and their parameters while typing in a command string.

Command Line Edit

Command line edit allows non-destructive cursor movements on a command already typed.

Table 5 Command Line Edit Commands

Key Stroke	Description
(Ctrl B) or left arrow	Go back one character.
(Ctrl F) or right arrow	Go forward one character.
(Esc B)	Go back one word.
(Esc F)	Go forward one word.
(Ctrl A)	Go to beginning of command.
(Ctrl C)	Discontinues (or kills) the currently running CLI process.

Table 5 Command Line Edit Commands

Key Stroke	Description
(Ctrl E)	Go to end of command.
(Ctrl K)	Delete all characters after the cursor.
(Ctrl D)	Delete one character.

Command Retrieval *Command retrieval* lists the history of commands previously entered. Use the history command to display the current command history.

You can change the number of commands kept in the command history buffer using [set command](#) with the history argument.

Table 6 Command History Retrieval Commands

Parameter	Description
(Ctrl P) or up arrow	Recall previous command in history list.
(Ctrl N) or down arrow	Recall next command in history list.

Positional Help *Positional help* displays the list of possible parameters when you enter the ? character (question mark) after any command or parameter. It then re-displays the line you typed, without the ?, so you can enter the parameter you wish to use. This helps you find the parameter you need and add it to your command, without having to retype the entire command string. Be sure to leave a space between the keyword and the question mark when using positional help.

Command Completion The TAB key provides *command completion*. When you press the TAB key before finishing typing a command or parameter, the rest of the command or parameter is displayed (completed), and you can continue entering the command. If the command or parameter is ambiguous, the bell dings, and the display does not change.

Output Pause When output to your screen pauses because more than 24 lines are waiting for display, you can press ENTER to display one more *line of output*, Space to display *one more page* of output, or q to *quit* the command.

Ending a Process The Ctrl C key combination discontinues the current running process. For other ways to terminate processes, refer to [kill](#).

Administrative Commands

This section covers administrative commands of the CLI.

help This command provides command explanations and information about their formats. Entering *only* `help` lists all possible commands. Entering `help <command name>` lists the possible parameters for that command.

Typing part of a keyword (command or parameter) and pressing Tab completes the keyword. If you have not yet entered enough of the keyword for it to be unique, pressing Tab causes the bell to ring and does not auto-complete.

Entering ? (question mark) after a command string displays the possible keywords and values for that command.

Syntax

```
help
help <command name>
show ?
```

Example

```
help set ip
```

history This command displays previously entered CLI commands. Recall commands from the history cache by using Ctrl P to recall commands up the list, and Ctrl N to recall commands working down the list.

The default depth is 10 commands and the configurable range is 1 to 500. You can modify history depth using [set command](#) with the `history <number>` parameter.

Syntax

```
history
```

Example

```
history
```

Related Commands

[set command](#)

kill This command kills an active process. Use [list processes](#) to view active processes. You can only kill a process that you started, and processes are killed by the process name—you can not kill by index number.



You must type upper case letters and the full process name when issuing the `kill` command.

Syntax

```
kill <process name>
```

Example

```
kill ping
```

Related Commands

[list processes](#)

[set command](#)

reboot This command reboots the system. If you have made any configuration changes, be sure to issue the [save all](#) command before rebooting.

Syntax

```
reboot
```

Example

```
reboot
```

Related Commands

[save all](#)

save all This command saves all changes made during your CLI session. CommWorks recommends you save your changes frequently, just as you would with any other type of editor.

Syntax

```
save all
```

Example

```
save all
```

Related Commands

[reboot](#)

save configuration This command saves individual configuration files (.CFG) to a bulk configuration file for uploading to the access router card. Name the bulk configuration file with the [set bulk_file](#) command.

The [reset](#) command with the configuration parameter breaks out individual configuration files from the bulk configuration file.

Syntax

```
save configuration
```

Example

```
save configuration
```

Related Commands

[delete configuration](#)

[reset](#)

[set bulk_file](#)

Date and Time Commands

Date and time commands manage date and time properties assigned to the access router card.

set date This command sets the system date, and contains the option to set both the system date and system time (illustrated in the second syntax listing). Refer to the [set time](#) command to set only the system time and leave the system date unchanged.

Use [show date](#) and [show time](#) to see the current settings for the date and time.

Syntax:

```
set date <dd-mmm- [yy]yy>
```

```
set date <dd-mm- [yy]yy> time [hh:mm:ss]
```

Table 7 Set Date and Time Parameters

Parameter	Description	Range
dd	The numeric date of the month.	Any valid date.
mmm	The first three letters of the month.	Any of the 12 months.
[yy]yy	The year expressed in 2 or 4 digits.	1997 to 2036
hh	The numeric setting of the hour on a 24-hour clock.	0 to 24
mm	The numeric setting of the minutes.	0 to 59
ss	The numeric setting of the seconds (optional).	0 to 59

Example:

```
set date 01-JAN-02 time 10:15:00
```

Related Commands

[set time](#)

[show date](#)

[show time](#)

set time This command sets the system time in Greenwich Mean Time (GMT) and leaves the date unchanged. Use [show date](#) to view current settings. The format is *hh:mm:ss*. The seconds field is optional. The [set date](#) command also sets the time.

Syntax

```
set time <hh:mm:ss>
```

Example

```
set time 15:15:00
```

Related Commands

[show date](#)

[set date](#)

set timezone This command sets the local time zone. This time zone can be a simple time zone rule or the name of one of the pre-defined time zone names. To see a list of the pre-defined time zones, use the [list timezone](#) command. All of the standard BSD Unix time zones are supported in the router card.

The local clock adjusts its time offset depending on the time zone settings. The `show ntp settings` command displays the current active time zone along with other information.

Syntax

```
set timezone <timezone>
```

Example

```
set timezone GMT
```

Related Commands

[list timezone](#)

list timezone This command displays a listing of available timezones to assign using [set timezone](#).

Syntax

```
list timezone
```

Example

```
list timezone
```

Related Commands

[set timezone](#)

show date This command displays the current system date, time, and uptime. The present time is expressed in Greenwich Mean Time (GMT).

Syntax

```
show date
```

Example

```
show date
```

Related Commands

[set date](#)

show time This command displays the current system date, time, and uptime. The present time is expressed in Greenwich Mean Time (GMT).

Syntax

```
show time
```

Example

```
show time
```

Related Commands

[set time](#)

Bulk File Commands

Bulk file commands handle the configuration files stored on the access router card.

set bulk_file This command specifies the name of a router card bulk configuration file, which is the compressed concatenation of individual the router card configuration files (.CFG) used for uploading to the router card.

You can name one of two bulk configuration files with the set bulk_file command and break out individual configuration files from the bulk configuration file with the [reset](#) command.

Syntax

```
set bulk_file <filename>
```

Example

```
set bulk_file myfile.cfg
```

Related Commands

[reset](#)

[show bulk_file](#)

show bulk_file This command displays the name of the router card bulk configuration file and any error associated with the file. This binary file is a concatenation of individual router card configuration files (.CFG) used to upload to the router card.

Syntax

```
show bulk_file
```

Example

```
show bulk_file
```

Related Commands

[set bulk_file](#)

Chat Script Commands

Chat script commands are used to add, delete, verify, list, and show chat scripts.

add chat_script This command adds the specified file to the router card's chat script table. Chat scripts are helpful for general-purpose scripting by dial-in users.

A chat script file must first be created using either the edit command or an off-line editor. Creating the file internally stores it in the router card's Flash memory. If the file is created off-line, you must create a TFTP client on the router card using the add tftp client command and TFTP the file to FLASH.



The `add chat_script` command must be issued before a chat script can run for a RADIUS user whose Vendor Specific Attribute refers to this file. Also, multiple users can reference the same chat file.

Syntax

```
add chat_script <name>
```

Example

```
add chat_script <script_name>
```

Related Commands

[delete chat_script](#)

[list chat_scripts](#)

[show chat_script](#)

[verify chat_script](#)

Refer to the *Total Control 1000 Enhanced Data System Operations Guide* for more information about chat script syntax, constructs, and use with RADIUS.

verify chat_script

This command verifies the syntax of the specified file previously added to the Chat Script table. This command is useful when a file has been edited and requires that its syntax be checked. For more information see the *Total Control 1000 Enhanced Data System Operations Guide* for more information.

Syntax

```
verify chat_script <name>
```

Example

```
verify chat_script script5
```

Related Commands

[add chat_script](#)

[delete chat_script](#)

[list chat_scripts](#)

[show chat_script](#)

delete chat_script Removes the specified file from the chat script table. For more information, refer to the add, verify, show and list chat_scripts commands. Also, see *The Total Control 1000 Enhanced Data System Operations Guide* for more information.

Syntax

```
delete chat_script <filename>
```

Example

```
delete chat_script script5
```

Related Commands

[add chat_script](#)

[list chat_scripts](#)

[show chat_script](#)

[verify chat_script](#)

list chat_scripts This command displays the name and status of chat script files you added to the chat script table.

Syntax

```
list chat_scripts
```

Example

```
list chat_scripts
```

Related Commands

[add chat_script](#)

[delete chat_script](#)

[show chat_script](#)

[verify chat_script](#)

Refer to the *Total Control 1000 Enhanced Data System Operations Guide* for more information.

show chat_script This command displays the entire chat script file you added to the chat script table. Refer to *The Total Control 1000 Enhanced Data System Operations Guide* for more information.

Syntax

```
show chat_script <name>
```

Example

```
show chat_script script5
```

Related Commands

[add chat_script](#)

[delete chat_script](#)

[list chat_scripts](#)

[verify chat_script](#)

Page Break Commands

Page break commands control page break display appearance on the terminal for locally and globally connected users.

enable command global_terminal_ settings_page_breaks

This command allows an administrative (*manage*) user to *globally* (for all router card sessions) enable page breaks for commands which display text—list, show, etc.—that would otherwise overflow the boundaries of the display screen. Alternatively, you can enable page breaks *locally* for a manage user's session with the [enable command local terminal settings page breaks](#) command.

Syntax

```
enable command global_terminal_settings_page_breaks
```

Example

```
enable command global_terminal_settings_page_breaks
```

Related Commands

[set command](#)

[disable command global_terminal_settings_page_breaks](#)

[disable command local_terminal_settings_page_breaks](#)

**disable command
global_terminal_
settings_page_breaks**

This command disallows (for admin CLI users) page breaks (more processing) for all users. Alternatively, you can disable page breaks locally for a manage user's session with [disable command local terminal settings page breaks](#).

Syntax

```
disable command global_terminal_ settings_page_breaks
```

Example

```
disable command global_terminal_ settings_page_breaks
```

Related Commands

[enable command global_terminal_ settings_page_breaks](#)

[enable command local_terminal_settings_page_breaks](#)

[set command](#)

**enable command
local_terminal_settings_
page_breaks**

This command allows an administrative (manage) user to locally (for the present session only) enable page breaks for commands which display text—list, show, etc.—that would otherwise overflow the boundaries of the display screen. Alternatively, you can enable page breaks *globally* with the [enable command global terminal settings page breaks](#) command.

Syntax

```
enable command local_terminal_settings_page_breaks
```

Example

```
enable command local_terminal_settings_page_breaks
```

Related Commands

[set command](#)

[disable command global_terminal_ settings_page_breaks](#)

[disable command local_terminal_settings_page_breaks](#)

**disable command
local_terminal_settings
_page_breaks**

This command disallows (for admin CLI users) page breaks (more processing) for locally (the present session only) connected users. Alternatively, you can disable page breaks globally for a manage user's session with the [disable command global terminal settings page breaks](#) command.

Syntax

```
disable command local_terminal_settings_page_breaks
```

Example

```
disable command local_terminal_settings_page_breaks
```

Related Commands

[disable command global terminal settings page breaks](#)

[enable command global terminal settings page breaks](#)

[enable command local terminal settings page breaks](#)

[set command](#)

Set Commands

This section covers set commands

set command

This command configures the command line parameters.

Syntax

```
set command  
global_terminal_settings_rows <number>  
history <number>  
idle_timeout <interval>  
local_prompt <string>  
local_terminal_settings_rows <number>  
login_required [no | yes]  
prompt <string>
```

Table 8 Set Command Parameter Descriptions

Parameter	Description
global_ terminal_ settings_rows	Configures the page size (number of rows) output by CLI commands to subsequent the router card-connected sessions of administrative (manage) users. This command is not effective for currently connected users. The range is 1-256. The default is 23.
history	Sets depth of the buffer holding command history. Use history command to see current depth and list of your last CLI commands. The default is 10 commands. The range is 1-500.
idle_timeout	Sets Console login connection to close after being idle for the specified interval, if that user is required to log in (login_required value must be set to YES. The range is 0-60 minutes. The default is 5 min. Zero (0) value produces no timeout. This value can be changed only by a manage user.
local_prompt	Sets a separate (temporary) prompt for a command file session. The limit is 64 ASCII characters.
local_ terminal_ settings_rows	Configures the page size (number of rows) output by CLI commands to locally connected PC screens of administrative (manage) users. This command is effective only for the session when the command is issued. The range is 1-256. The default is 23.
login_required	Sets whether a user on the Console port is required to log in. This value can be changed only by a manage user. The default is No.
prompt	Sets the global (permanent) command prompt for the CLI. Use show command to see the currently defined prompt. The limit is 64 ASCII characters.

set system This command specifies system information displayed using the show system command.

Syntax

```
set system
    name <name>
    location <location>
    contact <contact information>
    transmit_authentication_name <keyword>
    dialin_transmit_password <user_password>
```

The transmit authentication name is used when the router card receives a challenge—typically during LAN to LAN or L2TP/PPTP routing—while making a PPP connection to a remote system/router over the WAN (PPP requires a user at the datalink layer, which you supply here).

Table 9 Set System Command Parameter Descriptions

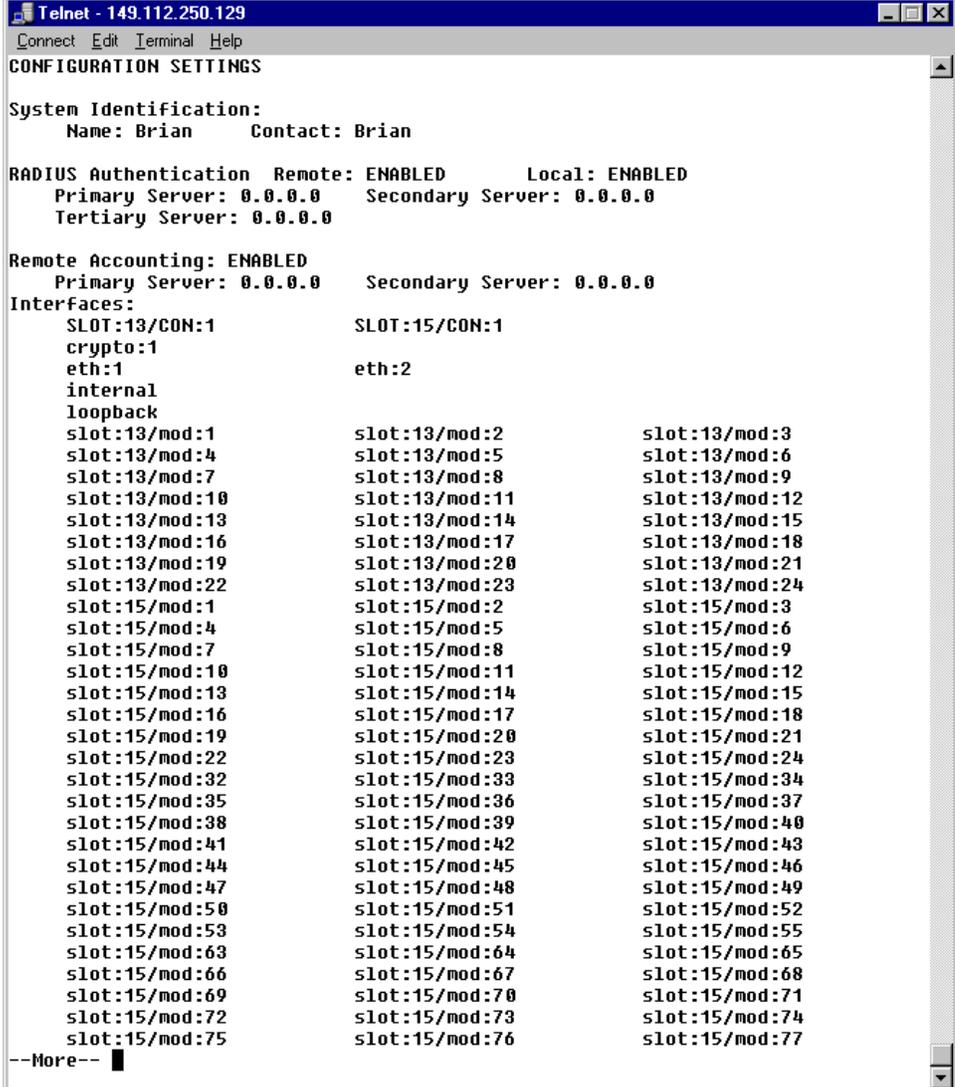
Parameter	Description	Range
name	The designation of your access router card.	Up to 64 ASCII characters.
location	The site of the router card.	Up to 64 ASCII characters.
contact	The name of the router card administrator.	Up to 64 ASCII characters.
transmit_authentication_name	Remote account name. Note: In LAN-to-LAN and L2TP/PPTP connections, this name must match the user name at the far end of the connection.	Up to 64 ASCII characters.
dialin_transmit_password	Establishes the system wide password which is used for authenticating the access router card to the peer for dialin connections. Default is null.	Up to 64 ASCII characters.

show all configuration output

This command executes a [do](#) script in the Flash file system called 'showall.cnf'. The 'showall.cnf' file is compiled into netserve.dmf and is installed automatically. If the filename argument is supplied, the command output is re-directed to the file instead of standard output to the CLI.

Syntax

```
show all configuration output <filename>
```

Figure 2 Configuration Settings Output


```
Telnet - 149.112.250.129
Connect Edit Terminal Help
CONFIGURATION SETTINGS

System Identification:
  Name: Brian      Contact: Brian

RADIUS Authentication Remote: ENABLED      Local: ENABLED
  Primary Server: 0.0.0.0      Secondary Server: 0.0.0.0
  Tertiary Server: 0.0.0.0

Remote Accounting: ENABLED
  Primary Server: 0.0.0.0      Secondary Server: 0.0.0.0

Interfaces:
  SLOT:13/CON:1              SLOT:15/CON:1
  crypto:1
  eth:1                      eth:2
  internal
  loopback
  slot:13/mod:1              slot:13/mod:2              slot:13/mod:3
  slot:13/mod:4              slot:13/mod:5              slot:13/mod:6
  slot:13/mod:7              slot:13/mod:8              slot:13/mod:9
  slot:13/mod:10             slot:13/mod:11             slot:13/mod:12
  slot:13/mod:13             slot:13/mod:14             slot:13/mod:15
  slot:13/mod:16             slot:13/mod:17             slot:13/mod:18
  slot:13/mod:19             slot:13/mod:20             slot:13/mod:21
  slot:13/mod:22             slot:13/mod:23             slot:13/mod:24
  slot:15/mod:1              slot:15/mod:2              slot:15/mod:3
  slot:15/mod:4              slot:15/mod:5              slot:15/mod:6
  slot:15/mod:7              slot:15/mod:8              slot:15/mod:9
  slot:15/mod:10             slot:15/mod:11             slot:15/mod:12
  slot:15/mod:13             slot:15/mod:14             slot:15/mod:15
  slot:15/mod:16             slot:15/mod:17             slot:15/mod:18
  slot:15/mod:19             slot:15/mod:20             slot:15/mod:21
  slot:15/mod:22             slot:15/mod:23             slot:15/mod:24
  slot:15/mod:32             slot:15/mod:33             slot:15/mod:34
  slot:15/mod:35             slot:15/mod:36             slot:15/mod:37
  slot:15/mod:38             slot:15/mod:39             slot:15/mod:40
  slot:15/mod:41             slot:15/mod:42             slot:15/mod:43
  slot:15/mod:44             slot:15/mod:45             slot:15/mod:46
  slot:15/mod:47             slot:15/mod:48             slot:15/mod:49
  slot:15/mod:50             slot:15/mod:51             slot:15/mod:52
  slot:15/mod:53             slot:15/mod:54             slot:15/mod:55
  slot:15/mod:63             slot:15/mod:64             slot:15/mod:65
  slot:15/mod:66             slot:15/mod:67             slot:15/mod:68
  slot:15/mod:69             slot:15/mod:70             slot:15/mod:71
  slot:15/mod:72             slot:15/mod:73             slot:15/mod:74
  slot:15/mod:75             slot:15/mod:76             slot:15/mod:77

--More--
```

- do** This command runs a script file from Flash memory, which contains a series of CLI commands. The output parameter is optional.

Syntax

```
do <input_filename> output <output_filename>
```

cfp_delay_command Use this command in [do](#) scripts to force a delay before a command is executed. This command is useful when performing two consecutive add commands.

Syntax

```
cfp_delay_command <number>
```

Related Commands

[do](#)

set board command_line_ parameters

This command specifies CLI arguments used prior to the router card boot up. You can issue a command at the CLI to begin configuration using the bulk configuration file you earlier TFTPd into the router card's Flash memory. This command is useful when performing similar configurations on multiple router cards.

Syntax

```
set board command_line_parameters <string>
```

Example

```
set board command_line_parameters anyname.cfg
```

Related Commands

[show board command_line_parameters](#)

set bootrom boot interface

This command selects the Ethernet interface (LAN interface number) to use for booting over the LAN. Use the [list lan interfaces](#) command to display available Ethernet interfaces. Because this parameter is used only at system boot up and is directly written into EEPROM, the [save all](#) command is not required to save it.

Syntax

```
set bootrom boot interface <eth:x>
```

Related Commands

[list lan interfaces](#)

[save all](#)

set bootrom config

This command sets bootrom parameters (used only at system boot up). The bootmode refers to a boot image taken from system Flash memory or an image taken from a host on the network. The IP configuration source is where the network configuration is derived from during *network* booting, either *statically* (from the router card) or from a network host via the *bootp* method. Because these parameters are written to EEPROM directly, the [save all](#) command is not required to save them.

Syntax

```

set bootrom config
    bootmode [flash | network]
    ip_config_source [bootp | static]
    upload_crashdump [disable | enable]

```

Table 10 Set Bootrom Command Parameter Descriptions

Parameter	Description
bootmode	Sets booting method from Flash memory or the <i>network</i> . Default: Flash.
ip_config_source	If booting over the LAN, IP parameters will be taken either from <i>static</i> configuration in the board or will use <i>bootp</i> . Default: Static.
upload_crashdump	If the system crashes, it uploads the crash dump file to the configured tftp server. Default: Disable

set bootrom ip interface

This command sets IP parameters for each LAN interface (used only when the system boots up). These IP parameters are used for network downloading of the image during booting and uploading crash dump information to a network host. Because the parameters are written to EEPROM directly, the [save all](#) command is not required to save them.

Syntax

```

set bootrom ip interface <eth:x>
    address <IP address>
    crashdump_file <filename>
    gateway <IP address>
    loadfile <filename>
    netmask <IP netmask>
    tftpserver <IP address>
    tftp_boot [always | never | once]

```

Table 11 Set Bootrom IP Interface Command Parameter Descriptions

Parameter	Description
<eth:x>	LAN interface address
address	The IP address of the interface
crashdump_file	Crashdump information is written in to this file in the TFTP server. The limit is 127 ASCII characters.
Gateway	IP address of the router card.
Loadfile	File name of system boot image kept in the TFTP server. The limit is 127 ASCII characters.

Table 11 Set Bootrom IP Interface Command Parameter Descriptions

Parameter	Description
Netmask	Netmask of the LAN interface.
tftpserver	IP address of the host from which the boot image is to be downloaded and crash dump information is to be uploaded.
tftp_boot	How often boot image is downloaded from tftp server. This parameter is valid only if bootmode is set to NETWORK. The choices are: <ul style="list-style-type: none"> ■ NEVER—NETWORK boot will <i>not</i> be attempted. Default ■ ONCE—boots from NETWORK <i>once</i>; after that bootmode changes to FLASH. ■ ALWAYS—each time the system boots, the image is taken from the network.

CLI Exit Commands

The following commands are available to dial-in (modem) and Telnet (LAN) users so they can disconnect from the CLI.

quit This command exits the CLI, but keeps this connection open. These commands return you to the dial-in user or Telnet commands.

Syntax

```
quit
```

Example

```
quit
```

logout This command exits the CLI and closes the connection. This ends the dial-in user or Telnet session.

Syntax

```
logout
```

Example

```
logout
```

leave This command exits the CLI.

Syntax

```
leave
```

Example

```
leave
```

EEPROM

EEPROM commands deal with information stored on the access router card's EEPROM.

**delete board
crashdump**

This command removes the last crashdump saved on the router card.

Syntax

```
delete board crashdump
```

Example

```
delete board crashdump
```

show board crashdump

A diagnostic tool for displaying information about a previous system crash stored in EEPROM. This is useful for debugging purposes only. Information shown includes the router card version number, general purpose and other registers, and call stacks.

Syntax

```
show board crashdump
```

Example

```
show board crashdump
```

**disable system
reset_eeprom**

This command disallows inclusion of earlier-saved EEPROM configuration when performing a bulk configuration download. The default is disabled.

Syntax

```
disable system reset_eeprom
```

Example

```
disable system reset_eeprom
```

Related Commands

[enable system reset_eeprom](#)

[reset](#)

[show system](#)

**enable system
reset_eeprom**

This command applies earlier-saved EEPROM configuration when performing a bulk configuration download. EEPROM settings are saved in the bspman.cfg file when a save all is performed. This file and configured filter files are saved in the bulk configuration file when a save configuration command is issued. This command applies these saved EEPROM settings back into the router card when the bulk configuration file is downloaded and a reset configuration command is issued. The default is disabled.



CAUTION: *CommWorks recommends that you not use this command unless you are an expert user.*

Syntax

```
enable system reset_eeprom
```

Example

```
enable system reset_eeprom
```

Related Commands

[disable system reset_eeprom](#)

[reset](#)

[save all](#)

[show system](#)

**Event Logging
Commands**

This section covers event logging commands available in the CLI.

add syslog

This command adds IP host to the list of IP hosts that receives syslog entries. You can see the current log levels for the system using [list facilities](#), and modify the current loglevel for each facility using set facility loglevel.



All SYSLOG messages generated by the Auth facility are sent regardless of loglevel set. To modify this function, disable the allow_all_auth_levels parameter. All other router card facilities are sent only if their loglevels match the configured syslog loglevel.

Syntax

```
add syslog <IP address>

    allow_all_auth_levels [yes | no]

    buffer count <1 to 256>

    facility [log_auth | log_local0 | log_local1 | log_local2
log_local3 | log_local4 | log_local5 | log_local6 |
log_local7]

    loglevel [critical | unusual | common | verbose]
```

Table 12 Add Syslog Command Parameter Descriptions

Parameter	Description
<ip_name_or_address>	Host name or IP address of the UNIX host that will receive SYSLOG information.
allow_all_auth_levels	Permits or denies transmission of all loglevel syslog messages by the Auth facility. The default is Yes .
buffer_count	The size of the buffer to save the last event information sent to the syslog server. The range is 1 to 256 .
facility	The SYSLOG node facility (site) where SYSLOG messages are sent. See choices above. The default is log_auth .
loglevel	There are four levels of logging: <ul style="list-style-type: none"> ■ CRITICAL—a serious system error, which may effect system integrity. Default ■ UNUSUAL—an abnormal event, which the system should be able to recover from ■ COMMON—a regularly occurring event ■ VERBOSE—a regular periodic event, e.g. a routing update message

Related Commands[list facilities](#)

delete syslog This command removes the specified IP host name or address from the list of addresses which are authorized to receive SYSLOG information. Use [list syslogs](#) to see the currently allowed addresses.

Syntax

```
delete syslog <IP name or address>
```

Example

```
delete syslog 10.10.3.49
```

Related Commands[list syslogs](#)

disable icmp logging This command disables display of the Internet Control Message Protocol (ICMP) to the SYSLOG server. Use [show icmp](#) to view edits. ICMP is disabled by default.

Syntax

```
disable icmp logging
```

Example

```
disable icmp logging
```

Related Commands

[enable icmp logging](#)

[show icmp](#)

disable syslog event_log This command disables syslog event buffering.

Syntax

```
disable syslog event_log
```

Example

```
disable syslog event_log
```

enable syslog event_log This command enables syslog event buffering.

Syntax

```
enable syslog event_log
```

Example

```
enable syslog event_log
```

reset syslog event_log This command resets the syslog event log counters back to zero.

Syntax

```
reset syslog event_log
```

Example

```
reset syslog event_log
```

enable icmp logging This command enables display of the ICMP to the SYSLOG server, providing feedback about routing, diagnostic, or error messages encountered by IP. ICMP is disabled by default.

Syntax

```
enable icmp logging
```

Example

```
enable icmp logging
```

Related Commands

[disable icmp logging](#)

[show icmp](#)

list syslogs This command displays IP addresses which get SYSLOG entries from the Syslog Table.

Syntax

```
list syslogs
```

- **Syslog**—IP address to which syslog entries will be sent.
- **Log Level**—Reporting level of entries to send: (e.g.) *UNUSUAL*.
- **M(e)s(sa)g(e)**—Current number of messages sent since system bootup.
- **Count**—Number of event messages sent to this SYSLOG sink.
- **Facility**—SYSLOG sink node facility to which the SYSLOG message is sent. Values displayed are LOG_AUTH, LOG_LOCAL0, LOG_LOCAL1, LOG_LOCAL2, LOG_LOCAL3, LOG_LOCAL4, LOG_LOCAL5, LOG_LOCAL6, and LOG_LOCAL7.
- **Allow All Auth Levels**—Permits or denies transmission of all loglevel SYSLOG messages by the Auth facility. The default is Yes.

Related Commands

[add syslog](#)

[delete syslog](#)

[list facilities](#)

[set facility](#) (controls output to console port)

set facility Sets the severity reporting level of a facility to display messages on the console (your hard-wired connection to the router card) or on a PC telneted to the router card. Use the [list facilities](#) command to view the current loglevel for each facility. Default loglevels for most facilities is *critical*.



Do not confuse set facility and set syslog commands. The set facility command determines which messages are generated on the console or to a telneted PC—depending on the loglevel specified for each facility. The set syslog command, on the other hand, determines which messages are saved—depending on the global loglevel you’ve set for the particular SYSLOG host.

Syntax

```
set facility <name> loglevel [critical | unusual | common |
verbose | debug]
```

Related Commands

[list facilities](#)

show events This command displays event messages on the console if a telnet connection is established to the router card.

Syntax

```
show events
```

The log levels are:

- **Critical**—A serious system error, which may effect system integrity.
- **Unusual**—An abnormal event from which the system should recover.
- **Common**—A regularly occurring event.
- **Verbose**—A regular periodic event, e.g. a routing update message.
- **Debug**—For debugging purposes only.

Related Commands

[list facilities](#)

[set syslog](#)

[show events](#)

set syslog This command sets the error reporting level and the destination for SYSLOG entries sent to the specified host. You must have previously defined this syslog IP address using the [add syslog](#) command.

Syntax

```
set syslog <IP address>
    allow_all_auth_levels [yes | no]
    facility [log_auth | log_local0 | log_local1 | log_local2 |
log_local3 | log_local4 | log_local5 | log_local6 |
log_local7]
    loglevel [critical | unusual | common | verbose]
    buffer_count <1 to 256>
    buffer_reset [yes | no]
```

Table 13 Set Syslog Command Parameter Descriptions

Parameter	Description	Range
IP address	The syslog's IP address where information is directed.	xxx.xxx.xxx.xxx
allow_all_auth_levels	Permits or denies transmission of all loglevel SYSLOG messages by the Auth facility. The default is Yes .	yes no
facility	SYSLOG facility where output is sent. See choices above. The default is log_auth.	log_auth log_local0 to log_local7
loglevel	SYSLOG loglevel to which output is assigned.	critical—a serious system error, which may effect system integrity. Default. Unusual—An abnormal event, from which the system should recover. Common—A regularly occurring event. Verbose—A regular periodic event, e.g. a routing update message.
buffer_count	The buffer size to save the last event information sent to the syslog server.	1 to 256
buffer_reset	Reset the syslog server's event buffer on the router card.	yes no



All Syslog messages generated by the Auth facility are sent regardless of loglevel set. To modify this function, disable the allow_all_auth_levels parameter. All other router card facilities are sent only if their loglevels match the configured syslog loglevel.



Do not confuse the set facility and set syslog commands. The set facility command determines which messages are generated on the console or to a

telneted PC—depending on the loglevel specified for each facility. The set syslog command, on the other hand, determines which messages are saved—depending on the global loglevel you’ve set for the particular Syslog host.

set syslog_format This command sets the format for the system log.

Syntax

```
set syslog_format [default | format_one]
```

- default—Use the default standard format for the system log.
- format_one—Use the non-standard format for the system log. Gives more information on the reasons the Telnet/ClearTCP calls were terminated.

show syslog This command shows information for the specified syslog server.

Syntax

```
show syslog <IP name or address>
```

Table 14 Show Syslog Fields and Descriptions

Fields	Description	Range
IP name or address	The network name or IP address of the syslog server.	xxx.xxx.xxx.xxx

show syslog_format This command displays the setting of the format for the system log which was set using [set syslog_format](#).

Syntax

```
show syslog_format
```

- default—Use the default standard format for the system log.
- format_one—Use the non-standard format for the system log. Gives more information on the reasons the Telnet/ClearTCP calls were terminated.

Syntax

```
show syslog_format
```

Related Commands

[set syslog_format](#)

Event Commands

- disable**
critical_events_to_flash
- This command disables logging all critical errors to sinks and Flash memory, avoiding the problem of too many critical errors generating a Flash overload. Be aware of the following conditions:
- The error log file is automatically renamed when the router card reboots.
 - Critical messages are still output to the console.
 - Issuing the [save all](#) command preserves this setting in the configuration file.

Syntax

```
disable critical_events_to_flash
```

Use the [show critical event settings](#) command to view logging configuration and event sinks. The default is disabled.

Related Commands

[save all](#)

[show critical_event settings](#)

[enable critical_events_to_flash](#)

- enable**
critical_events_to_flash
- This command enables logging all critical errors into all sinks and Flash memory. Issue this command when a Flash overload due to many critical errors is *not* anticipated. Be aware that the error log file is *not* automatically renamed when the router card reboots. Issuing the [save all](#) command preserves this setting in the configuration file. Use the [show critical event settings](#) command to view logging configuration and event sinks.

The default is disabled.

Syntax

```
enable critical_events_to_flash
```

Related Commands

[save all](#)

[show critical_event settings](#)

[disable critical_events_to_flash](#)

hide events This command reverses the [show events](#) command by which all events being directed to the console or syslog are also echoed to the Telnet session you are running.

Syntax

```
hide events
```

Related Commands

[show events](#)

list critical events This command displays the last *ten* critical status events, the facility at issue, the system time when each occurred, and a description of the event. You can change which events are logged as critical, using the [set facility](#) command.

Syntax

```
list critical events
```

Related Commands

[enable critical_events_to_flash](#)

[set facility](#)

show events This command displays all events being directed to the console to also be echoed to the Telnet or dial-in session you are running. Any number of users can employ this function. The [hide events](#) command ends this directive. Use the [set facility](#) command to set the event level.

Syntax

```
show events
```

Related Commands

[hide events](#)

[set facility](#)

IP Network Commands

This section covers commands to add, delete, list, and configure IP network settings using the CLI.

delete ip source route This command deletes the specified source route from the routing table. Specify the source route by its network name or IP address.

Syntax

```
delete ip source route <IP name or address>
```

Table 15 Show Syslog Fields and Descriptions

Fields	Description	Range
IP name or address	The network name or IP address of the syslog server.	xxx.xxx.xxx.xxx

list ip addresses This command displays the IP address for each active IP network.

Syntax

```
list ip addresses
```

- **Address**—IP address of the interface.
- **Bcast Algo**—Algorithm used to determine which address to broadcast representing the entire network. Choices are:
 - **1**—the IETF standard: xxx.xxx.xxx.255 (default)
 - **0**—the BSD standard: xxx.xxx.xxx.000
- **Reassembly Max Size**—Maximum allowable size of packet that can be reassembled from a fragmented packet.
- **Interface**—Interface this IP address uses to connect to the system. Values displayed are internal, loopback, eth:1, or eth:2.

list ip defaultroute This command displays default gateway IP routers, which act as default routes for IP packets destined for remote hosts unknown to the router card. All unspecified routes are automatically sent to this gateway.

A default route gateway specified with a higher metric acts as the primary default route gateway and a second default route gateway with a lower metric acts as the secondary default route gateway. It lists the following information.

Syntax

```
list ip defaultroute
```

- **address**—IP address of the default route
- **Mask**—Subnet mask of the default route
- **Gateway**—IP address of the gateway router
- **Metric**—Hop count to the gateway
- **State**—Status of the default route

reconfigure ip network This command automatically reconfigures IP network parameters of an established static IP LAN network. This command changes network parameters without the administrator having to remove the router from service by manually disabling the network, modifying its parameters and re-enabling it. This command modifies *static* IP LAN networks only (cannot change interface and frame values for an *internal* address).

Syntax

```
reconfigure ip network <network name>
    address <IP address>
    interface <eth:1 | eth:2>
    frame [ethernet_ii | snap | atm1483 | atm1577]
    wan_type [unntp | nntp | network]
    remote_address <remote IP address and mask>
```

Related Commands

[add ip network](#)

[delete ip network](#)

[disable ip network](#)

[enable ip network](#)

[list ip networks](#)

[set ip network <name>](#)

[show ip network <network_name> settings](#)

Monitoring Protocols

Use the protocol monitor facility in the router card to monitor the realtime activity of routing protocols.

monitor protocol

This command launches the utility for monitoring realtime protocol activity. A menu is displayed as shown below. Enter the letter that designates the desired protocol you want to monitor.

Syntax

```
monitor protocol
```

The following information displays:

```
HiPer PROTOCOL Monitor
Select a letter for one of the following options:
A) Monitor PPTP
B) Monitor L2TP
C) Monitor PPPoE
D) Monitor ISAKMP
X) Exit the monitor
Please Enter Your Choice:
```

- Monitor PPTP or L2TP allows you to:
 - **Monitor a particular tunnel**—choosing this option prompts the user to enter the IP Address of the tunnel endpoint of the tunnel that needs to be monitored.
 - **Monitor tunnel to a particular IP address**—choosing this option prompts the user to enter the IP Address of the tunnel endpoint of the tunnel that needs to be monitored. Once the tunnel endpoint is filled, user is prompted for session related options.
 - **Monitor the next tunnel**—choosing this option lets the user monitor the next tunnel to come up. This option prompts the user for session related options.
- **Monitor PPPoE** allows you to:
 - **Monitor all packets**—Choosing this option allows you to monitor all PPPoE packets, including discovery stage and session packets.
 - **Monitor Discovery Stage packets**—Choosing this option allows you to monitor the packets passed during the discovery stage of the PPOE session.
 - **Monitor Session Stage packets**—Choosing this option allows you to monitor all PPPoE packets once a PPPoE session has been established.
- **Monitor ISAKMP** allows you to:
 - **Monitor All ISAKMP packets**—Choosing this option allows you to monitor all ISAKMP packets.

- **Monitor All ISAKMP packets between specified endpoints**—Choosing this option allows you to monitor packets between a specified local address and a specified remote address.

There are two types of display styles: decoded (default) and hex dump.

In the decoded mode, the packets are displayed in a textual format. Pressing capital X or H switches the display style to hex dump. Pressing capital D switches the display back to decoded mode.

Show All Commands

show all configuration settings

This command shows the complete configuration of the system as determined by the commands in the *showall.cnf* configuration file that is supplied with the netserve.dmf binary image.



Depending on your connection, this may take several minutes to load. There is a lot of information to display.

Syntax

```
show all configuration settings
```

show all active interfaces

This command displays setting information for all active interfaces.

Syntax

```
show all active interfaces
```

show all connections

This command displays all current connections.

Syntax

```
show all connections
```

show all filters This command displays all filters currently being used.

Syntax

```
show all filters
```

show all interfaces This command displays details for all interfaces.

Syntax

```
show all interfaces
```

show all ip networks This command displays details for all configured IP networks.

Syntax

```
show all ip networks
```

show all ipx networks This command displays details for all configured IPX networks.

Syntax

```
show all ipx networks
```

show all l2tp tunnels This command displays details of all L2TP tunnels.

Syntax

```
show all l2tp tunnels
```

show all lan interfaces This command displays details for all configured LAN interfaces.

Syntax

```
show all lan interfaces
```

show all networks This command displays details for all configured networks.

Syntax

```
show all networks
```

show all ospf areas This command displays details of all configured OSPF areas.

Syntax

```
show all ospf areas
```

show all ospf interfaces This command displays the details of all configured OSPF interfaces.

Syntax

```
show all ospf interfaces
```

show all sessions This command displays information for all sessions.

Syntax

```
show all sessions
```

show all switched interfaces This command displays the information for all switched interfaces.

Syntax

```
show all switched interfaces
```

show all users This command displays various parameters for different types of users such as login, network, tunnel, and network PPP users.

Syntax

```
show all users
```

Related Commands

[list users](#)

[show user](#)

show all vpn This command displays the following information on VPN tunnels.

Syntax

```
show all vpn <number> vtp tunnels
```

- **Tunnel Id**—A unique value for a tunnel.
- **Interface**—Indicates an interface on which call arrived.
- **VpnId**—Indicates the VPN the user is connected to.
- **VpnName**—The name of the VPN the user is connected to.
- **PeerIpAddress**—On the VPNGW this indicates the respective NAS. On the NAS this points to the IP address of the VPNGW to which the user is connected.
- **EstablishedTime**—The time the VTP tunnel was established.

show all vtp tunnels This command displays the following information for all VTP tunnels.

Syntax

```
show all vtp tunnels
```

- **Tunnel Id**—A unique value for a tunnel.
- **Interface**—Indicates an interface on which call arrived.
- **VpnId**—Indicates the VPN the user is connected to.
- **VpnName**—The name of the VPN the user is connected to.
- **PeerIpAddress**—On the VPNGW this indicates the respective NAS. On the NAS it points to the IP address of the VPNGW to which the user is connected.
- **EstablishedTime**—This is the time the VTP tunnel was established.

Show Commands Show commands display detailed information about a specific table entry or a set of scalars (non-table items).

show board command_line_parameters This command displays command line arguments used at boot time.

Syntax

```
show board command_line_parameters
```

Related Commands

[set board command_line_parameters](#)

show board settings This command displays information about the router card hardware.

Syntax

```
show board settings
```

show bootrom settings This command displays general boot configuration.

Syntax

```
show bootrom settings
```

Table 16 Show Bootrom Settings Display Information

Settings	Description	Range
Boot Mode	Identifies where the access router card acquires a boot image from.	Flash TFTP
IP Configuration Source	Displays which method the access router card uses to obtain an IP address.	Static DHCP
Crash Upload	Sets uploading of crash dump information.	enabled disabled
Boot Interface	Displays which interface the card is configured to use upon bootup.	eth:1 eth:2

Related Commands

[set bootrom config](#)

show command settings

This command displays the settings for CLI commands.

Syntax

```
show command settings
```

Table 17 Show Command Settings Display Information

Setting	Description	Range
History Depth	Number of CLI commands issued by the router card which display when pressing the up or down arrow keys.	1 to 500
Current Prompt	Designation of prompt for a temporary CLI session.	Up to 64 ASCII characters
Local Prompt	Designation of prompt for a permanent CLI session.	Up to 64 ASCII characters
Console Login Required	Whether login to the console is required.	yes no
Console Idle Timeout	Interval before a console session is timed out.	0 to 60
Global Terminal Page Break	Whether global terminal page breaks are enabled or disabled.	enabled disabled
Global Terminal Settings Rows	Number of rows displayed to all the router card-connected systems.	1 to 256
Local Terminal Page Break	Whether local terminal page breaks are enabled or disabled.	enabled disabled
Local Terminal Settings Rows	Number of rows displayed to locally-connected systems.	1 to 256

Related Commands

[set command](#)

show configuration settings

This command displays a variety of system information including system, network, protocol, interface, forwarding, routing, DNS, host and datalink parameters.

Syntax

```
show configuration settings
```

show cpu utilization This command displays an estimate of the router card's CPU usage over various intervals, derived from an estimate of how quickly the router card polls under load versus the polling rate of the router card not under load. The router card uses excess processing power to lower system throughput latency. If the router card is not running for the respective time period, the CPU percentage would be represented as 0%.

Syntax

```
show cpu utilization
```

show date This command displays the system date, time, and uptime. The time is expressed in Greenwich Mean Time (GMT).

Syntax

```
show date
```

Related Commands

[set date](#)

show file This command displays the contents of the specified ASCII file. To view the contents of a specified hexadecimal file, use the second syntax.

Syntax

```
show file <filename>  
show file <filename> hex
```

show maximum_local_users This command displays the maximum number of users that can be created locally on the router card.

Syntax

```
show maximum_local_users
```

show memory This command displays the router card's DRAM (Dynamic Random Access Memory) usage.

Syntax

```
show memory
```

- **Total System Memory Resources**—Total amount of usable memory for router applications.
- **Free Memory**—Amount of memory not in use.
- **Code Size**—Amount of memory used by code.
- **Initialized Data Size, Uninitialized Data Size, Stack Size**—Static data areas.

show memory utilization This command displays system DRAM memory usage resources as well as periodic memory usage checks. It lists the following information:

- **Total System Memory Resources**—Total amount of usable memory for router applications.
- **Free Memory**—Amount of memory not in use.
- **Code Size**—Amount of memory used by code.
- **Initialized Data Size, Uninitialized Data Size, Stack Size**—Static data areas.
- **Free Memory Current Value**—Amount of memory currently not in use.
- **Free Memory 1 Hour Before**—Amount of memory not in use one hour ago.
- **Free Memory 12 Hour Before**—Amount of memory not in use 12 hours ago.
- **Free Memory 24 Hour Before**—Amount of memory not in use 24 hours ago.
- **Total Buffer Cache**—The total number of cache buffer entries reserved in the system. The unit is *number of entries*. Each entry in the buffer cache contains a buffer header that contains a pointer to the actual data and has a data structure of 40 bytes.
- **Free Buffer Cache**—The number of buffer cache entries available. The unit is *number of entries*. Each entry in the buffer cache contains a buffer header that contains a pointer to the actual data and has a data structure of 40 bytes.

show network This command displays the configured settings for the specified network. For an example, see the output from the show ip network command.

Syntax

```
show network <name>
```

show packet_logging This command displays settings for packet size and logging.

Syntax

```
show packet_logging settings
```

Related Commands

[set_packet_logging](#)

show remote user This command Displays settings for the specified user, currently connected to the router card. Settings displayed vary with the type of user connected.

Syntax

```
show remote user <username>
```

- **User Name**—Name of the currently connected user
- **Service Type**—Type of network service employed by the user: *Login, Framed, Callback, Dialout, Administrative*
- **NAS IP Address**—IP address of the router card
- **NAS Port**—Port attribute of the router card
- **Login Ip Host**—IP address of the host this user is currently logged into
- **Login Service**—Type of login service employed by this user: *Telnet, RLogin, TCP, Ping*
- **Login Port**—Port number on the router card where this user is connected
- **State**—Value returned by RADIUS server (in Access-Challenge packet) during CHAP authentication
- **Class**—Value returned by RADIUS server (in Access-Challenge packet) during CHAP authentication
- **Session Timeout**—Interval in seconds this user has to remain connected before being timed out
- **Idle Timeout**—Interval in seconds this user has to remain idle before being timed out
- **Port Limit**—Maximum number of dial-in ports a user can concurrently employ
- **Min(imum) Compression size**—The minimum packet size for which compression is to be done

- **Port Tap**—Indicates whether the Port Tap feature is enabled or not
- **Port Tap Format**—Indicates the Port Tap format type: *Hex(decimal), ASCII, Clear(TCP)*
- **Tap Output**—Indicates where output from the tap is destined: *Screen, Syslog*
- **Tap Facility**—End point where tap information can be directed
- **Tap Priority**—Preference levels of messages that can be logged: *Critical, Unusual, Common, Verbose*
- **Tap IP Address**—The IP address of the SYSLOG where Tap information is destined

Related Commands

[set user](#)

[add user](#)

show session This command displays the session configuration for the specified user.

Syntax

```
show session <user name>
```

- **Service Type**—Type of network service employed by the user: *Login, Framed, Callback, Dialout, Administrative*
- **Port Limit**—Maximum number of dial-in ports a user can concurrently employ
- **Session Timeout**—Interval in seconds this user has to remain connected before being timed out
- **Idle Timeout**—Interval in seconds this user has to remain idle before being timed out
- **Speed of Connection**—Estimate of the session's current bandwidth in bits per second.
- **NAS IP Address**—IP address of the router card
- **NAS Port**—Port attribute of the router card
- **State**—Value returned by RADIUS server (in Access-Challenge packet) during CHAP authentication
- **Class**—Value returned by RADIUS server (in Access-Challenge packet) during CHAP authentication
- **Login Ip Host**—IP address of the host this user is currently logged into
- **Login Service**—Type of login service employed by this user: *Telnet, RLogin, TCP, Ping*
- **Login Port**—Port number on the router card where this user is connected

show system This command displays system information.

Syntax

```
show system settings
```

- **System Descriptor**—Company designation of the router card including build date.
- **Object ID**—Identifies this system to SNMP managers.
- **System UpTime**—Time the system has been running since last boot.
- **System Contact**—Name of person responsible for system. Modify using **set system** command.
- **System Name**—Modify using set system command.
- **System Location**—Site where system is located. Modify using set system command.
- **System Services**—The type of service being provided.
- **System Transmit Authentication Name**—System-wide keyword for PPP on the WAN, modified using set system command.
- **System Version**—Loaded release version of the system software.
- **Reset EEPROM Settings On Bootup**—Whether earlier-saved EEPROM settings are reapplied upon bulk configuration download. The default is disabled.

Statistics

show statistics This set of commands displays statistical call and modem information.

Syntax

```
show statistics  
    call_disconnect_reasons  
    call_duration  
    call_statistics  
    calls_per_hour  
    modem_compression  
    modem_utilization  
    packets_forwarded_per_hour  
    ppp_download_packets  
    ppp_statistics  
    ppp_upload_packets  
    speed_statistics
```

Table 18 Show Statistics Command Parameter Descriptions

Parameter	Description
call_disconnect_reasons	Number of disconnect reasons for particular calls
call_duration	Number of calls with the following durations: Less than 1 minute Less than 2 minutes Less than 5 minutes Less than 10 minutes Less than 20 minutes Less than 1 hour: Less than 2 hours Less than 6 hours Less than 12 hours Less than 24 hours Less than 36 hours Greater than or equal to 36 hours
call_statistics	the Call statistics are based on the various characteristics of each call including: Number of OnDemand Connections Number of Dial Back Connections Number of Continuous Connections Number of Manual Connections Number of Timed Connections Number of Shared Connections Number of Dial-In Connections Number of Bond Connections Number of Dedicated Connections Number of Analog Calls Number of ISDN Calls Number of dial in users Number of Network users
calls_per_hour	the number of calls in an hour
modem_compression	the number of calls with different modem compressions used: No Modem Compression v.42bis Compression mnp5 Compression
modem_utilization	the percentage of utilization of the modem
packets_forwarded_per_hour	the number of packets forwarded per hour
ppp_download_packets	the number and size of ppp download packets
ppp_statistics	shows the PPP upload/download packet sizes, number of calls with different authentication scheme, etc.
ppp_upload_packets	the number of ppp upload packets in various packet sizes
speed_statistics	the number of calls with different speeds

reset This set of commands restores the router card settings to a default configuration.

Syntax

```

reset

    accounting counters

    accounting server_group [a | b] counters

    authentication counters

    configuration

    modem_group <name>

    modems <slot:x/mod:[1-y],slot:x/mod:[1-y] . .

    pppoe counters

    resource_management counters

    dhcp_proxy counters

    l2tp session_counters

```

Table 19 Reset Command Parameter Descriptions

Parameter	Description
accounting counters	Restores accounting statistics to default values.
accounting server_group	Restores the accounting statistics for accounting server group A or B to the default values.
authentication counters	Restores authentication counters to default values.
configuration	Restores individual the router card configuration files (.CFG) from a bulk configuration file. The bulk configuration function reads all configuration files generated by the router card processes and concatenates them into a single compressed file which can then be uploaded by the Common Element Manager. A bulk configuration file can be named using the set bulk_file command.
modem_group	Resets the specified modem group following changes to its configuration. This "hard" reset issues an ATZ! command, closing any active connections on the ports.
modems	Resets the specified modems following changes to its configuration. This "hard" reset issues an ATZ! command, closing any active connections on that port. The command also lets you reset multiple modems. For example: reset modems slot:1/mod:[2-5],slot:2/mod:[7-9]
pppoe counters	Resets the PPPoE session counters.
resource_management counters	Resets the RADIUS resource management counters to zero.
dhcp_proxy counters	Resets DHCP Proxy counter
l2tp session_counters	Resets LTP2 Session Counter

Related Commands

[set_bulk_file](#)

reset statistics This set of commands resets the statistics listed in Table 20.

Syntax

```

reset statistics
    call_disconnect_reasons
    call_duration
    call_statistics
    modem_compression
    ppp_download_packets
    ppp_statistics
    ppp_upload_packets
    speed_statistics

```

Table 20 Reset Statistics Command Parameter Descriptions

Parameter	Description
call_disconnect_reasons	The number of disconnect reasons for particular calls
call_duration	The number of minutes each call lasted
call_statistics	The Call statistics are based on the various characteristics of each call including: Number of on-demand connections Number of dial-back connections Number of continuous connections Number of manual connections Number of timed connections Number of shared connections Number of dial-in connections Number of bond connections Number of dedicated connections Number of Analog Calls Number of ISDN Call Number of dial in users Number of Network users Number of Multi-link Connections
modem_compression	The number of calls with different modem compression used
ppp_download_packets	The number of ppp download packets
ppp_statistics	Shows the PPP upload/download packet sizes, number of calls with different authentication scheme, etc
ppp_upload_packets	The number of ppp upload packets
speed_statistics	The number of calls with different speeds

Session Commands

This section covers commands used to view session and session counter information.

list sessions This command displays information regarding current the router card connections.

Syntax

```
list sessions
```

- **Name**—Active session's user name.
- **Conn(ection) Type**—Active session's link type. LAN, WAN or UNKNOWN
- **Prot(ocol) Type**—Active session's protocol. PPP, SLIP, TELNET, RLOGIN, CLEARTCP or UNKNOWN

list sessions counters This command displays statistics regarding current the router card connections.

Syntax

```
list session counters
```

- **IfName**—The interface name
- **Conn(ection)Date**—The date the connection was made
- **Conn(ection)Time**—The time at which the connection was made
- **IdleTime**—Interval to wait before timing out an inactive connection
- **Bytes In**—Number of bytes received
- **Bytes Out**—Number of bytes sent

TCP Commands

This section covers commands used to view Transmission Control Protocol (TCP) information using the CLI.

show tcp counters This command displays system-wide TCP statistics.

Syntax

```
show tcp counters
```

- **Active Opens**—Number of times TCP connections have made a direct transition to SYN-SENT state from CLOSED state.
- **Passive Opens**—Number of times TCP connections have made a direct transition to SYN-RCVD state from LISTEN state.
- **Attempt Fails**—Number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.

- **Resets**—Number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
- **Currently Established**—Number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
- **Input Segments**—Sum of segments received.
- **Output Segments**—Sum of segments sent, including those on current connections but excluding those containing only retransmitted octets.
- **Retransmitted Segments**—Sum of segments retransmitted.
- **Dropped ahead of seq segments**

PPP Commands

This section covers commands used to view Point to Point Protocol (PPP) information.

show ppp on interface <slot:x/mod:y> counters

This command displays statistics for PPP running on the specified interface when interface is active.

Syntax

```
show ppp on interface <slot:x/mod:y> counters
```

Counters For PPP Bundle

- **Operational Status**—Whether it is opened or not opened.
- **Number Active Links**—Sum of active links using this PPP bundle.
- **Transmit Packets**—Sum of packets transmitted over this bundle.
- **Bytes from Upper Layer**—Sum of bytes received from an upper layer application for transmission over this bundle. This counter represents all data handed down to the PPP application BEFORE compression occurs.
- **Bytes to Lower Layer**—Sum of bytes sent to a lower layer application for transmission over this bundle. This counter represents all data to be handed down to the lower layer application AFTER compression occurs.
- **Received Packets**—Sum of packets received from a lower layer application over this bundle.
- **Bytes to Upper Layer**—Sum of bytes to be handed up to an upper layer application over this bundle.
- **Bytes from Lower Layer**—Sum of bytes received from a lower layer application over this bundle.
- **Total Bad Headers**—Sum of packets with incorrect PPP Header (address, Control, PID Field).

Counters For PPP Link

- **Operational Status**—Whether it is opened or not opened
- **Received Packets—Too Long**—Sum of frames judged too long.

- **Transmit Frames**—Sum of frames received from the PPP application for transmission over this link.
- **Bytes from Upper Layer**—Sum of bytes handed down from an upper layer application for this link.
- **Bytes to Lower Layer**—Sum of bytes received from a lower layer application for this link.
- **Received Frames**—Sum of frames received on this link.
- **Bytes to Upper Layer**—Sum of bytes handed up to an upper layer application over this link.
- **Bytes from Lower Layer**—Sum of bytes received from a lower layer application over this link.

UDP Commands

This section covers commands used to view User Datagram Protocol (UDP) information using the CLI.

list udp listeners

This command displays local IP address and port number for each UDP port being used by the system. These ports correspond to processes that are receiving UDP data (for example SNMP, User Management, TFTP service).

Syntax

```
list udp listeners
```

show udp counters

This command displays statistics for UDP datagrams.

Syntax

```
show udp counters
```

Input Counters

- **Total Input Datagrams**—Sum of UDP datagrams received.
- **Input but No Port**—Sum of received UDP datagrams for which there was no application at the destination port.
- **Input with other Errors**—Sum of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

Output Counters

- **Total Output Datagrams**—Sum of UDP datagrams sent.

VTP Commands

This section covers Virtual Terminal Protocol (VTP) commands of the CLI.

show vtp This command displays VTP information for counters, settings, or tunnels.

Syntax

```
show vtp
    counters
    settings
    tunnel <tunnel number>
```

- **Counters**—The following counters are defined and displayed for VTP.
 - Vtp Registration Requests received
 - Vtp Registration Requests sent
 - Vtp Registration Responses received
 - Vtp Registration Responses sent
 - Vtp Refresh Requests received
 - Vtp Refresh Requests sent
 - Vtp Refresh Responses received
 - Vtp Refresh Responses sent
 - Vtp Deregistration Requests received
 - Vtp Deregistration Requests sent
 - Vtp Deregistration Responses received
 - Vtp Deregistration Responses sent
 - Vtp PDU Authentication Failures
 - Vtp VPN Validation Failures
 - Vtp Timestamp Failures
- **Settings**—Displays the state of time stamp checking, either enabled or disabled.
- **Tunnel**—Displays the following information for the specified VTP tunnel:
 - **Tunnel Id**: A unique value for a tunnel.
 - **Interface**: Indicates an interface on which call arrived.
 - **VpnId**: Indicates the VPN the user is connected to.
 - **VpnName**—Name of the VPN the user is connected to.
 - **PeerIpAddress**—On the VPNGW this indicates the respective NAS. On the NAS it points to the IP address of the VPNGW to which the user is connected.

- **EstablishedTime**—This is the time the VTP tunnel was established.

Accounting

show accounting counters

This command displays statistics stored by RADIUS accounting servers.

Syntax

```
show accounting counters
```

- **Number Of Local Users**—Number of LAN users RADIUS is tracking.
- **Number of Active Users**—Sum of users RADIUS is tracking.
- **UDP Packets Received**—Number of packets received from RADIUS.
- **UDP Packets Retransmitted**—Number of packets sent to RADIUS.
- **Round Robin switching count**—Number of times servers are switched in each server group.
- **Percent Queue Full**—Portion of the queue filled in each server group.
- **Number of Packets Outstanding**—Sum of packets left by each server group.
- **Number of Packets Discarded**—Sum of packets thrown away by each server group.

show accounting server_group [a | b] counters

This command displays statistics stored by the primary (a) or secondary (b) RADIUS accounting servers. This command displays the following information.

Syntax

```
show accounting server_group [a | b] counters
```

- **Server's IP Address**—The IP address of the server.
- **Average Roundtrip Time**—The average time in milliseconds it takes information to get to the server and back.
- **Accounting Requests**—The total number of RADIUS Accounting-Request packet sent since client (the access router card) start-up. This does not include retransmissions.
- **Accounting Retransmissions**—The total number of RADIUS Accounting-Request packets retransmitted to the same server since client (the access router card) start-up. Retransmissions include retries where the Identifier and Acct-Delay have been updated.
- **Accounting Responses**—The total number of RADIUS Accounting-Response packets received from this server since client (the access router card) start-up.
- **Malformed Accounting Responses**—The total number of malformed RADIUS Accounting-Response packets received from this server since client

(the access router card) start-up. Bad authenticators are not included as malformed access responses.

- **Accounting Bad Authenticators**—The total number of RADIUS Accounting-Response packets which contained invalid authenticators received from this server since client (the access router card) start-up.
- **Accounting Timeouts**—The total number of accounting timeouts to this server since client (the access router card) startup. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
- **Client Unknown Type**—The total number of RADIUS packets of unknown type which were received from this server on the accounting port since client (the access router card) start-up.

ATM Commands

show atm counters This command displays statistics for all ATM interfaces.
[ds3:x | e3:x | atmcell:x]

Syntax

```
show atm counters [ds3:x | e3:x | atmcell:x]
```

Authentication Commands

This section covers Remote Access Dial-in User Authentication commands of the CLI.

show authentication settings This command displays the RADIUS and local user authentication settings.

Syntax

```
show authentication settings
```

- **Local Authentication**—Displays status of local authentication settings. The default is enabled.
- **Remote Authentication is**—Displays status of remote authentication settings. The default enabled.
- **Hint Assigned is**—Displays status of hint assigned settings. The default is disabled.
- **Primary Server is**—Displays the Primary Server's IP address. The default value is 0.0.0.0.
- **Primary Destination Port is**—Displays current primary destination port.
- **Secondary Server is**—Displays the Secondary Server's IP address. The default value is 0.0.0.0
- **Secondary Destination Port is**- Displays current secondary destination port.

- **Tertiary Server is**—Displays the Tertiary Server's IP address. The default value is 0.0.0.0.
- **Tertiary Destination Port is**—Displays current tertiary destination port.
- **Source Port is**—Displays the source port.
- **Retransmission Timeout**—Displays current timeout settings. The default is 3 seconds.
- **Max Retransmissions**—Displays the maximum number of re-transmissions. The default is 10.
- **Per Server Retry Count**—Displays the current retry count per server. The default is 3.
- **Vendor Specific Attribute**—Displays the status of the vendor specific attribute setting. The default is enabled.
- **Prioritize Auto Server**—Displays the current setting of the Prioritize Authentication Servers. The Default is disabled.
- **Active Authentication Server**—Displays the IP address of the active Authenticating Server.
- **Send service type indication**—Displays the send service type indication settings. The default is enabled.
- **Authentication Counters Systoles**—Displays Authentication Counters Syslogs settings. The Default is disabled.
- **Authentication Counters Syslog Frequency**—Displays Authentication Counters Syslog Frequency. The default is TWELVE HOURS.
- **Authentication Counters Syslog Reset**—Displays Authentication Counters Syslog Reset settings. The default is disabled.
- **Primary Auth Server Preference**—Displays the preference of the Primary Authentication Server. Default is 1.
- **Secondary Auth Server Preference**—Displays the preference of the secondary Authentication Server. Default is 2.
- **Tertiary Auth Server Preference**—Displays the preference of the Tertiary Authentication Server. Default is 3.

show authentication counters

This command displays the RADIUS and local user authentication counters.

Syntax

```
show authentication counters
```

- **Local Successful Authentications**—Number of times user/password pair matched.
- **Local Failed Authentications**—Number of times user/password pair didn't match.
- **Remote Primary Successful Authentications**—Number of times RADIUS Okayed user on this server.

- **Remote Primary Failed Authentications**—Number of times RADIUS rejected user on this server.
- **Remote Secondary Successful Authentications**—Number of times RADIUS Okayed user on this server.
- **Remote Secondary Failed Authentications**—Number of times RADIUS rejected user on this server.
- **Remote Tertiary Successful Authentications**—Number of times RADIUS Okayed user on this server.
- **Remote Tertiary Failed Authentications**—Number of times RADIUS rejected user on this server.
- **Remote Primary No Responses**—Number of times RADIUS failed to answer an authentication request (with an error message) on this server.
- **Remote Secondary No Responses**—Number of times RADIUS failed to answer an authentication request (with an error message) on this server.
- **Remote Tertiary No Responses**—Number of times RADIUS failed to answer an authentication request (with an error message) on this server.

**show authentication
server_status**

This command shows the settings as well as the current status of all the servers.

Syntax

```
show authentication server_status
```

**Connection
Commands**

This section covers commands used to view connection and connection counters.

**show connection
settings**

This command displays the settings for dial-in connections.

Syntax

```
show connection settings
```

- **Host Selection Method**—ROUND-ROBIN or RANDOM.
- **Global User Name**—USR_NETS is the global user name, used when no other is available.
- **Service Prompt**—The prompt displayed when a dial-in user is connected.
- **Manage Prompt**—The prompt shown to a dial-in manage user on login.
- **Banner File Name**—The name of the file which contains the connection banner message.
- **Global Connect Message**—The message users see when they are first connected.

- **Manage User Dialin Access**—Whether administrative access is allowed through dial-in ports.
- **Command Prompt**—The prompt displayed when users dial in.
- **Login Host Connect Timeout**—A specified period of time (in seconds) in which the systems tries to establish connection for login users. As soon as login users are authenticated, the access router card tries to connect the login user to its login host.
- **Login Connection Buffering**—Enables and disables data buffering. If data buffering is enabled, it buffers all the data from the user, after authentication phase until the connection establishment phase for login user.

Related Commands

[set connection](#)

show connection counters

This command displays the *Counter For Connections*, kept for dial-in connections, displays the number of incoming calls.

Syntax

```
show connection counters
```

DNS Commands

This section covers Domain Name Server display commands.

show dns counters

This command displays various counters for DNS.

Syntax

```
show dns counters
```

- **Total Queries Received**—Sum of DNS queries received.
- **Total Response Sent**—Sum of DNS responses sent.
- **Responses from Client Processing**—DNS responses from local DNS Host Table.
- **Responses from Server Processing**—DNS responses from the DNS Server Table.
- **Success Responses from Server**—Successful responses to DNS requests.
- **Error Response sent**—Sum of failures to DNS requests, specifics shown below.

Specific Error Counters

- **Format Errors**—Number of Format Error responses received by DNS.
- **Problems with Name Server**—Internal server error.

- **NonExistent Name**—Number of times the requested name could not be resolved.
- **Server refused the request**—Server was able to accept a request.
- **Server does not implement request**—Server was able to accept a request.
- **Corrupted Responses**—Response did not decrypt.
- **Timeouts**—Number of time outs waiting for the server to respond.
- **Response could not be sent**—The requester had terminated.
- **Non-authoritative Data Responses**—Number of requests made by the resolver for which a non-authoritative answer (cached data) was received.
- **Non-authoritative No Data Responses**—Number of requests made by the resolver for which a non-authoritative answer—no such data response (empty answer) was received.
- **Martians**—Number of responses received which were received from servers that the resolver does not think it asked.
- **Received Responses**—Number of responses received to all queries.
- **Unparseable Responses**—Number of responses received which were unparseable.
- **Fallbacks**—Number of times the resolver had to fall back to its seat belt information.
- **Good Caches**—Number of resource records the resolver has cached successfully.
- **Bad Caches**—Number of resource records the resolver has refused to cache because they appear to be dangerous or irrelevant. For example, resource records with suspiciously high TTLs, unsolicited root information, or those that don't appear to be relevant to the question the resolver asked.
- **Good Negative Caches**—Number of authoritative errors the resolver has cached successfully.
- **Bad Negative Caches**—Number of authoritative errors the resolver would have liked to cache but was unable to because the appropriate Resource Record was not supplied or looked suspicious.

Frame Relay Commands

This section covers frame relay interface commands of the CLI.

**show frame_relay
interface
<interface_name>
counters**

This command displays statistics of the DLL created on top of the physical WAN interface.

Syntax

```
show frame_relay interface <interface_name> counters
```

- **Transmitted Frames**—Sum of frames transmitted on this interface
- **Transmitted Octets**—Sum of bytes transmitted on this interface
- **Received Frames**—Sum of frames received on this interface
- **Received Octets**—Sum of bytes received on this interface
- **Unknown Errors**—Sum of errors whose cause is unexplained
- **Received Short Frames**—Sum of errors caused by the reception of frames that were not long enough to allow de-multiplexing—the address field was incomplete, or for virtual circuits using Multiprotocol over Frame Relay, the protocol identifier was missing or incomplete.
- **Received Long Frames**—Sum of frames exceeding the maximum length configured for this interface
- **Illegal DLCIs**—Sum of errors caused by the reception of LMI status frames containing illegal DLCIs.
- **Unknown DLCIs**—Sum of link maintenance frames containing an Information Element type invalid for the configured link maintenance protocol.
- **Protocol Errors**—Unspecified error occurred when attempting to interpret link maintenance frame.
- **Link Faults**—The number of times the interface has gone down since it was initialized.
- **Last Fault Time**—The system up time in days, minutes, hours and seconds at the time when the interface was taken down due to excessive errors. Excessive errors is defined as the time when a DLL exceeds the *Error Threshold* number within *Monitored Events* interval.

**show frame_relay
interface
<interface_name> lmi
statistics**

This command displays Link Management Interface statistics of the DLL created on top of the physical WAN interface as specified by the *interface_name* parameter.

Syntax

```
show frame_relay interface <interface_name> lmi statistics
```

LMI Protocol Statistics

- **LMI Tx Frames**—Sum of LMI packets transmitted by this DLL
- **LMI Rx Frames**—Sum of LMI packets received by this DLL
- **LMI Tx Status Enquiry Frames**—Sum of LMI Status Enquiry frames transmitted by this DLL
- **LMI Rx Status Enquiry Frames**—Sum of LMI Status Enquiry frames received by this DLL
- **LMI Tx Status Frames**—Sum of LMI Status frames transmitted by this DLL
- **LMI Rx Status Frames**—Sum of LMI Status frames received by this DLL
- **LMI Rx Status Update Frames**—Sum of LMI Status Update frames received by this DLL
- **No Response From Network Count**—Number of LMI Status Enquiry frames that were unanswered by the network side

LMI Protocol Error Counters

- Invalid Q.922 Header
- Invalid Control Field
- Invalid Protocol Discriminator Field
- Invalid Call Reference Field
- Invalid Message Type Field
- Invalid Locking Shift IE
- Invalid Report Type IE
- Invalid Link Integrity Verification IE
- Invalid Sequence Number
- Invalid PVC Status IE

LMI Received Unsolicited Message

- Unrecognized IE
- LMI Incomplete Message
- Out Of Order IE
- Invalid Spare Bits
- Invalid Extension Bit

- Invalid New, Active or Delete Bits

show frame_relay pvc <pvc_name> counters

This command displays statistics of the specified Frame Relay PVC.

Syntax

```
show frame_relay pvc <pvc_name> counters
```

- **Tx Frames To Driver**—Sum of frames sent to a physical driver during the transmit action by this PVC since it was created.
- **Tx Octets To Driver**—Sum of bytes sent to a physical driver during the transmit action by this PVC since it was created.
- **Tx Frames From Forwarders**—Sum of frames received from forwarders during the transmit action by this PVC since it was created.
- **Tx Octets From Forwarders**—Sum of bytes received from forwarders during the transmit action by this PVC since it was created.
- **Tx Frames Congested By Driver**—Sum of frames congested by a physical driver during the transmit action by this PVC since it was created.
- **Tx Octets Congested By Driver**—Sum of bytes congested by a physical driver during the transmit action by this PVC since it was created.
- **Tx Frames Discarded By FR PVC**—Sum of frames discarded during the transmit action by this PVC since it was created.
- **Tx Octets Discarded By FR PVC**—Sum of bytes discarded during the transmit action by this PVC since it was created.
- **Rx Frames From Driver**—Sum of frames received from a physical driver by this PVC since it was created.
- **Rx Octets From Driver**—Sum of bytes received from a physical driver by this PVC since it was created.
- **Rx Frames By Forwarders**—Sum of frames handed down from forwarders to this PVC since it was created.
- **Rx Octets By Forwarders**—Sum of bytes handed down from forwarders to this PVC since it was created.
- **Rx Frames Congested By Forwarders**—Sum of frames congested by forwarders during receive action by this PVC since it was created.
- **Rx Octets Congested By Forwarders**—Sum of bytes congested by forwarders during receive action by this PVC since it was created.
- **Rx Frames Discarded By FR PVC**—Sum of frames discarded during receive action by this PVC since it was created.
- **Rx Octets Discarded By FR PVC**—Sum of bytes discarded during receive action by this PVC since it was created.
- **Rx FECNs**—Sum of Forward Explicit Congestion Notifications received by this PVC since it was created.

- **Rx BECNs**—Sum of Backward Explicit Congestion Notifications received by this PVC since it was created.
- **Rx DEs**—Sum of frames received with DE bit set in the Q.922 header by this PVC since it was created.
- **Tx DEs**—Sum of frames sent with DE bit set in the Q.922 header by this PVC since it was created.
- **Tx IP Frames**—Sum of IP protocol frames sent by this PVC since it was created.
- **Rx IP Frames**—Sum of IP protocol frames received by this PVC since it was created.
- **Tx IPX Frames**—Sum of IPX protocol frames sent by this PVC since it was created.
- **Rx IPX Frames**—Sum of IPX protocol frames received by this PVC since it was created.
- **Tx AppleTalk Frames**—Sum of AppleTalk protocol frames sent by this PVC since it was created.
- **Rx AppleTalk Frames**—Sum of AppleTalk protocol frames received by this PVC since it was created.
- **Tx Bridged Frames**—Sum of bridged frames sent by this PVC since it was created.
- **Rx Bridged Frames**—Sum of bridged frames received by this PVC since it was created.
- **Creation Time**—Interval in days, hours, minutes and seconds since the specified PVC operational state was created.
- **Last Change Time**—Interval in days, hours, minutes and seconds since the specified PVC operational state was last changed.

Related Commands

[add frame_relay pvc](#)

[delete ip source route](#)

[disable frame_relay pvc](#)

[enable frame_relay pvc](#)

[set frame_relay pvc <pvc_name>](#)

**show datalink
frame_relay interface
<interface_name>
counters**

This command displays statistics of the DLL created on top of the physical WAN interface.

Syntax

```
show datalink frame_relay interface <interface_name> counters
```

- **Transmitted Frames**—Sum of frames transmitted on this interface.
- **Transmitted Octets**—Sum of bytes transmitted on this interface.
- **Received Frames**—Sum of frames received on this interface.
- **Received Octets**—Sum of bytes received on this interface.
- **Unknown Errors**—Sum of errors whose cause is unexplained.
- **Received Short Frames**—Sum of errors caused by the reception of frames that were not long enough to allow de-multiplexing—the address field was incomplete, or for virtual circuits using Multiprotocol over Frame Relay, the protocol identifier was missing or incomplete.
- **Received Long Frames**—Sum of frames exceeding the maximum length configured for this interface.
- **Illegal DLCIs**—Sum of errors caused by the reception of LMI status frames containing illegal DLCIs.
- **Unknown DLCIs**—Sum of link maintenance frames containing an Information Element type invalid for the configured link maintenance protocol.
- **Protocol Errors**—Unspecified error occurred when attempting to interpret link maintenance frame.
- **Link Faults**—The number of times the interface has gone down since it was initialized.
- **Last Fault Time**—The system up time in days, minutes, hours and seconds at the time when the interface was taken down due to excessive errors. Excessive errors is defined as the time when a DLL exceeds the *Error Threshold* number within *Monitored Events* interval.

**show datalink
frame_relay interface
<interface name> lmi
statistics**

This command displays link management interface statistics of the DLL created on top of the physical WAN interface specified by the `interface_name` parameter.

Syntax

```
show datalink frame_relay interface <interface name> lmi
statistics
```

LMI Protocol Statistics

- **LMI Tx Frames**—Sum of LMI packets transmitted by this DLL
- **LMI Rx Frames**—Sum of LMI packets received by this DLL
- **LMI Tx Status Enquiry Frames**—Sum of LMI Status Enquiry frames transmitted by this DLL
- **LMI Rx Status Enquiry Frames**—Sum of LMI Status Enquiry frames received by this DLL
- **LMI Tx Status Frames**—Sum of LMI Status frames transmitted by this DLL
- **LMI Rx Status Frames**—Sum of LMI Status frames received by this DLL
- **LMI Rx Status Update Frames**—Sum of LMI Status Update frames received by this DLL
- **No Response From Network Count**—Number of LMI Status Enquiry frames that were unanswered by the network side

LMI Protocol Error Counters

- Invalid Q.922 Header
- Invalid Control Field
- Invalid Protocol Discriminator Field
- Invalid Call Reference Field
- Invalid Message Type Field
- Invalid Locking Shift IE
- Invalid Report Type IE
- Invalid Link Integrity Verification IE
- Invalid Sequence Number
- Invalid PVC Status IE

LMI Received Unsolicited Message

- Unrecognized IE
- LMI Incomplete Message
- Out Of Order IE
- Invalid Spare Bits
- Invalid Extension Bit
- Invalid New, Active or Delete Bits

Chassis Commands This section covers commands used to view information on a chassis.

list chassis This command displays chassis settings for all slots.

Syntax

```
list chassis
```

show chassis slot <slot number> This command displays basic board information by slot number (1 to 16) in the chassis.

Syntax

```
show chassis slot <slot number> settings
```

show nmc status This command displays whether the NMC is present in the Total Control 1000 Chassis. When a query from the NMC to the router card is posted, its date and time are recorded.

Syntax

```
show nmc status
```

File Commands This section covers commands used to view, delete, list, rename, and copy files using the CLI.

delete configuration This command removes all your configuration files, reboots the system and restores system configuration to default values. For your protection, you are prompted to confirm the request.

Syntax

```
delete configuration
```

delete file This command deletes a file from the Flash file system. Use the list files command to see which files are currently stored.

Syntax

```
delete file <filename>
```

edit This command launches the router card's text editor. The edit command allows you to perform simple line editing of files, including filter files.

Edit is available on the Console, through a dialed-in connection, or via Telnet. It works best when displayed on an ANSI terminal since it employs escape sequences defined for the ANSI terminal type to clear screens and display menus. To access Help for this command, type a question mark (?) at the colon prompt (:).



Edit is especially convenient when creating small or editing large filter files. An alternative method uses TFTP but this method is more suited to creating large filter files.

Syntax

```
edit <input_file_name>
```

show critical_event settings This command displays where the log files for critical event messages are stored in Flash memory.

Syntax

```
show critical_event settings
```

- **Critical Event Sink**—Where critical events are logged, default is @file:./log-file.local
- **Critical Event Backup**—Where critical events are logged, if the first destination fails. The default is @file:./old-log-file.local.
- **Critical Event Logging To Flash**—indicates whether logging of all critical errors into all sinks and Flash is enabled or disabled.

copy file This command copies a file within the Flash file system. This is a flat file system.

Syntax

```
copy file <input_file> <output_file>
```

list files This command displays the files currently stored in the Flash file system. You can remove files using the delete file command, but you can add them via TFTP only.

Syntax

```
list files
```

rename file This command copies files within the Flash file system. The Flash file system is a flat file system (no subdirectories).

Use the [list files](#) command to view currently existing files. The <input file> is the name of the original file while the <output file> is the new name for the file.

Syntax

```
rename file <input_file> <output_file>
```

Related Commands

[list files](#)

show bulk_file This command displays name of the bulk configuration File and any bulk configuration errors.

Syntax

```
show bulk file
```

Network Commands This section covers commands used to view defined networks and counters.

list network This command displays all defined networks running any protocol.

Syntax

```
list network
```

- **Name**—Designation of the network that you defined with the add network command
- **Prot**—Protocol of the network: IP or IPX
- **Int**—Ethernet interface the network is running on: eth:1, eth:2, loopback, internal, slot:x/mod:y
- **State**—Condition of network: ENA (enabled), ENA* (enabling), DIS (disabled), DIS* (disabling), INIT (initialized), INV (*invalid*)
- **Type**—*STAT* (static), *DYN* (dynamic) or *AUTO* (default) network
- **Network address**—address of the IP network

show network <name> settings This command displays the settings for the specified network.

Syntax

```
show network <name> settings
```

show network <name> counters This command displays the statistical counters for the specified network. IP does not maintain network counters.

Syntax

```
show network <name> counters
```

Policy Commands This section covers commands to view IPsec policy information.

list policy This command list the IPsec policies currently loaded into the system cache.

Syntax

```
list policy
```

Processes and Facilities Commands This section covers commands to view process and facilities information.

list facilities This command displays the currently running system facilities (processes), plus the default log level, which represents the severity of error that facility outputs messages on the Console port. You can change the log level using the [set facility loglevel](#) command. By comparison, syslog log levels are specified by the [set syslog <name> loglevel](#) command.

Syntax

```
list facilities
```

Related Commands

[set facility](#)

[set syslog](#)

list processes This command displays all processes running on the system.

Syntax

```
list processes
```

It lists the following information:

- **Index**—A reference number in the Process Table
- **Name**—Designation of the process (e.g.: Domain Name System)
- **Type**—*SYSTEM*, *APPLICATION*, *FORWARDER* or *DRIVER*
- **Status**—*ACTIVE*, *PENDING* or *INACTIVE*

Routing Table Commands

This section covers commands for viewing information in the routing table.

list rtab preferred

This command displays routing table information.

Syntax

```
list rtab preferred
```

- **Destination**—IP network destination address.
- **Protocol**—The routing mechanism through which the specified route was discovered. The following values are displayed:
 - **RIP**—Any route discovered by RIP.
 - **REMOTE**—User-specified remote or IP Pool aggregated remote static route.
 - **LOCAL**—User-specified local route.
- **Age**—Time since route was created in seconds.
- **NextHop**—IP address of the next hop of the specified route.
- **Metric**—Number of hops between the router card and its destination.
- **Interface**—The router card Ethernet and modem interfaces to which the specified routes are mapped.

GRE Commands

This section covers commands for viewing Generic Routing Encapsulation (GRE) information.

show gre counters

Shows the statistics for GRE which is a layer between IP and VTP.

Syntax

```
show gre counters
```

These statistics include:

- GRE State
- Encapsulated Packets Received
- De-encapsulated Payloads Delivered
- De-encapsulated Payloads Discarded
- Packets Discarded Due To Malformed Header

- Packets Discarded Due To No Client
- Packets Received For Encapsulation
- Packets Encapsulated
- Packets For Encapsulation But Discarded
- Packets Encapsulated And Passed To IP

Health Trap Commands

Use health traps to get a continuous update of system utilization from the access router card. This can be used to obtain system utilization graphs on an hourly basis.

disable health_trap This command disables health traps.

Syntax

```
disable health_traps
```

enable health_trap This command enables health traps.

Syntax

```
enable health_traps
```

set health_trap interval This command sets the update interval in minutes, 1 to 1440.

Syntax

```
set health_trap interval
```

show health_trap This command displays the trap state and interval (in minutes).

Syntax

```
show health_trap settings
```

ICMP Commands

This section covers Internet Control Message Protocol (ICMP) commands of the CLI.

show icmp counters This command displays input and output counters for ICMP messages.



Traceroute-generated packets received by the router card will not increment the ICMP error counts Time Exceeded and Destination Unreachable. Also, a

number of ICMP error messages are sent to SYSLOG hosts while the Receive Destination Unreachable event is sent to the console.

Syntax

```
show icmp counters
```

Input Counters

- **Messages**—ICMP packets received.
- **Errors**—ICMP packets received with errors.
- **Destination Unreachable**—Sum of ICMP messages received when a router cannot forward a packet to its specified destination. *Error messages sent to the console and CLI.*
- **Time Exceeded**—Sum of ICMP messages generated by a router when time has exceeded or a timeout has occurred while waiting for a packet segment. *Error messages sent to SYSLOG host*
- **Parameter Problems**—Sum of ICMP messages generated by a router when it encounters an error. *Error messages sent to SYSLOG host*
- **Source Quench**—Sum of ICMP messages informing a host it should slow data transmission to ease congestion. *Error messages sent to SYSLOG host*
- **Redirects**—Sum of ICMP messages concerning a router advertising a host of a better next hop. *Error messages not logged*
- **Echos**—Sum of ICMP request messages received, signifying transport system success
- **Echo Replies**—Sum of ICMP reply messages received, indicating transport system success
- **Timestamps**—Sum of ICMP request messages received seeking time from another machine for clock synchronization and estimated transit time purposes. *Error messages sent to SYSLOG host*
- **Timestamp Replies**—Sum of ICMP timestamp reply messages
- **address Masks**—Sum of ICMP address Mask Reply messages. *Error messages sent to SYSLOG host*
- **address Mask Replies**—Sum of ICMP request messages concerning a host's ability to gather network information. *Error messages sent to SYSLOG host*
- **Advertise**—Sum of router advertisements received by the router card
- **Solicit**—Sum of host-generated router queries received by the router card. *Error messages sent to SYSLOG host.*

Output Counters

- **Messages**—Total of ICMP messages transmitted
- **Errors**—ICMP packets transmitted with errors

- **Destination Unreachable**—Sum of these messages sent. *Error messages sent to SYSLOG host*
- **Time Exceeded**—Sum of these messages sent. *Error messages sent to SYSLOG host*
- **Parameter Problems**—Sum of these messages sent. *Error messages sent to SYSLOG host*
- **Source Quench**—Sum of these messages sent
- **Redirects**—Sum of these messages sent. *Error messages sent to SYSLOG host*
- **Echos**—Sum of ICMP Echo (request) messages sent
- **Echo Replies**—Sum of these messages sent
- **Timestamps**—Sum of these messages sent
- **Timestamp Replies**—Sum of these messages sent
- **address Masks**—Sum of these messages sent
- **address Mask Replies**—Sum of these messages sent. *Error messages sent to SYSLOG host*
- **Advertise**—Sum of router advertisements sent by the router card. *Error messages sent to SYSLOG host*

Interface Commands

This section covers commands for viewing interface counters using the CLI.

show interface
<interface_name>
counters

This command displays counters for the specified interface.

Syntax

```
show interface <interface_name> counters
```

Input Counters

- **Octets**—Number of bytes received.
- **Ucast**—Number of unicast packets received.
- **MultiCast**—Number of multicast packets received.
- **BroadCast**—Number of broadcast packets received.
- **Discards**—Number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
- **Errors**—For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a number of inbound transmission units that contained higher-layer protocol.

- **Unknown Prot**—Number of unknown protocols in packet.

Output Counters

- **Octets**—Number of bytes transmitted.
- **Ucast**—Number of Unicast packets transmitted.
- **MultiCast**—Number of multicast packets transmitted.
- **BroadCast**—Number of broadcast packet transmitted.
- **Discards**—Number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
- **Errors**—For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.
- **Out QLen**—Length of the output packet queue (in packets).

IP Network Commands

This section covers commands for viewing information on IP networks.

show ip counters This command displays system-wide IP network statistics.

Syntax

```
show ip counters
```

Input Counters

- **Total Input Datagrams**—Sum of IP datagrams received
- **Bad Headers**—Number of datagrams with bad headers
- **Bad addresses**—Number of datagrams with bad addresses
- **Forwarded Packets**—Number of packets forwarded
- **Bad Protocol**—Number of packets received with bad protocol
- **Discarded**—Number of packets discarded
- **Successfully Delivered**—Number of packets successfully received

Output Counters

- **Total Output Datagrams**—Sum of datagrams transmitted
- **Discarded**—Number of datagrams discarded
- **Bad Routes**—Number of datagrams with a bad route
- **Fragments Needing Reassembly**—Number of fragmented datagrams

- **Datagrams Successfully Reassembled**—Number of fragmented datagrams successfully reassembled
- **Reassembly Failures**—Number of fragmented datagrams unsuccessfully reassembled
- **Datagrams Successfully Fragmented**—Datagrams successfully fragmented before transmission
- **Fragmentation Failures**—Failed datagram fragmentations before transmission
- **Total Fragments**—Sum of fragments transmitted

show ip rip counters This command displays RIP statistics.

Syntax

```
show ip rip counters
```

- **Received RIP Packets**—Number of rip packets received
- **Transmitted RIP Packets**—Number of rip packets transmitted
- **Received incorrect RIP Packets**—Number of rip packets incorrectly received

IPX Network Commands

This section covers commands used for viewing information on IPX networks.

show ipx counters This command displays the following counters for all IPX network activity.

Syntax

```
show ipx counters
```

Input Counters

- **Total Packets Received**—Sum of IPX packets received
- **Header Errors**—Sum of incoming packets discarded due to errors in their headers, including any IPX packet sized less than a minimum of 30 bytes
- **Unknown Sockets**—Sum of incoming packets discarded because the destination socket was not open
- **Discarded**—Sum of incoming packets discarded due to reasons other than those accounted for by Header Errors, and Unknown Sockets
- **Checksum Errors**—Sum of IPX packets received with wrong checksums
- **Delivered Locally**—Sum of IPX packets delivered locally, including packets from local applications
- **No Route to Destination**—Number of times no route to a destination was found

- **Too Many Hops**—Sum of incoming packets discarded for exceeding the hop count
- **Filtered Out**—Sum of incoming packets filtered out
- **Decompression Errors**—Sum of incoming packets discarded due to compression errors

Output Counters

- **Total Packets Transmitted**—Sum of IPX packets transmitted
- **Forwarded Packets**—Sum of IPX packets forwarded
- **Local Transmits**—Sum of IPX packets transmitted to local hosts
- **Local Malformed Transmits**—Sum of IPX packets supplied locally containing structural errors
- **Discarded**—Sum of outgoing packets discarded
- **Filtered Out**—Sum of packets filtered out before transmission
- **Compression Errors**—Sum of outgoing packets discarded due to compression errors
- **Socket Open Failures**—Sum of outgoing packets discarded because a socket was not available

**show ipx network
<network_name>
counters**

This command displays statistics for specified IPX network.

Syntax

```
show ipx network <network_name> counters
```

- **RIP Out Packets**—Sum of RIP packets transmitted
- **RIP In Packets**—Sum of RIP packets received
- **SAP Out Packets**—Sum of SAP packets transmitted
- **SAP In Packets**—Sum of SAP packets received

Related Commands

[add ipx network](#)

[delete ipx network](#)

[disable ipx network](#)

[enable ipx network](#)

[list ipx networks](#)

[show ipx network <network name> settings](#)

show ipx rip counters This command displays the sum of incorrect RIP packets.

Syntax

```
show ipx rip counters
```

show ipx sap counters This command displays the sum of incorrect SAP packets.

Syntax

```
show ipx sap counters
```

L2TP Tunnel Commands

This section covers Layer 2 Tunneling Protocol commands available in CLI.

show l2tp counters This command displays statistics for configured L2TP tunnels.

Syntax

```
show l2tp counters
```

- **Number of Active Tunnels**—Sum of currently active tunnels
- **Active Sessions**—Sum of currently active sessions
- **Fail Authentications**—Number of authentications failed by this L2TP stack since last initialized
- **Malformed Packets**—Sum of malformed packets received by this L2TP stack since last initialized
- **Control Tunnel Receive Packets**—Sum of control packets received by this L2TP stack since last initialized
- **Control tunnel receive packets with data**—Sum of control packets received with data by this L2TP stack since last initialized
- **Control tunnel receive packets without data**—Sum of zero length control packets received by this L2TP stack since last initialized
- **Processed control tunnel receive packets**—Sum of received control packets processed with data by this L2TP stack since last initialized
- **In sequence control tunnel receive packets**—Sum of control packets received in-sequence by this L2TP stack since last initialized
- **Out of sequence control tunnel receive packets**—Sum of control packets received out-of-sequence by this L2TP stack since last initialized
- **In order control tunnel receive packets**—Sum of control packets received in order by this L2TP stack since last initialized
- **Out of order control tunnel receive packets**—Sum of control packets received out-of-order by this L2TP stack since last initialized

- **Flow discarded control tunnel receive packets**—Sum of control packets discarded due to flow control by this L2TP stack since last initialized
- **Out of order discarded control tunnel receive packets**—Sum of control packets received and discarded due to ordering by this L2TP stack since last initialized
- **Control tunnel send packets**—Sum of control packets transmitted by this L2TP stack since last initialized
- **Control tunnel with data send packets**—Sum of control packets transmitted with data by this L2TP stack since last initialized
- **Control tunnel without data send packets**—Sum of zero length control packets transmitted without data by this L2TP stack since last initialized
- **Control tunnel flow control timeout**—Sum of control tunnel timeouts due to flow control experienced by this L2TP stack since last initialized
- **Local control tunnel flow control enables**—Sum of local control tunnel flow control enables experienced by this L2TP stack since last initialized
- **Remote control tunnel flow control enables**—Sum of remote control tunnel flow control enables experienced by this L2TP stack since last initialized
- **Control tunnel reassembly timeout**—Sum of control tunnel reassembly timeouts experienced by this L2TP stack since last initialized
- **Data tunnel receive packets**—Sum of data packets received by this L2TP stack since last initialized
- **Data tunnel with data receive packets**—Sum of data packets received with data by this L2TP stack since last initialized
- **Data tunnel without data receive packets**—Sum of zero length data packets received by this L2TP stack since last initialized
- **Processed data tunnel receive packets**—Sum of received data packets processed with data by this L2TP stack since last initialized
- **In sequence data tunnel receive packets**—Sum of data packets received in-sequence by this L2TP stack since last initialized
- **Out of sequence data tunnel receive packets**—Sum of data packets received out-of-sequence by this L2TP stack since last initialized
- **In order data tunnel receive packets**—Sum of data packets received in order by this L2TP stack since last initialized
- **Out of order data tunnel receive packets**—Sum of data packets received out-of-order by this L2TP stack since last initialized
- **Flow discarded data tunnel receive packets**—Sum of data packets discarded due to flow control by this L2TP stack since last initialized
- **Out of order discarded data tunnel receive packets**—Sum of data packets received and discarded due to ordering by this L2TP stack since last initialized

- **Data tunnel send packets**—Sum of data packets transmitted by this L2TP stack since last initialized
- **Data tunnel with data send packets**—Sum of data packets transmitted with data by this L2TP stack since last initialized
- **Data tunnel without data send packets**—Sum of zero length data packets transmitted without data by this L2TP stack since last initialized
- **Data tunnel flow control timeouts**—Sum of data tunnel timeouts due to flow control experienced by this L2TP stack since last initialized
- **Local data tunnel flow control enables**—Sum of local data tunnel flow control enables experienced by this L2TP stack since last initialized
- **Remote data tunnel flow control enables**—Sum of remote data tunnel flow control enables experienced by this L2TP stack since last initialized
- **Data tunnel reassembly timeouts**—Sum of data tunnel reassembly timeouts experienced by this L2TP stack since last initialized

NMC Commands

This section covers CLI commands that display information on the Network Management Card.

show nmc counters

This command displays DSA statistics for the NMC. This information is useful for debugging purposes.

Syntax

```
show nmc counters
```

OSPF Commands

This section covers Open Shortest Path First (OSPF) routing commands of the CLI.

show ospf area <area_id> counters

This command displays the specified OSPF area counters.

Syntax

```
show ospf area <area_id> counters
```

- **Area ID**—IP address of the OSPF area.
- **Area LSA Count**—Sum of link-state advertisements in this area's link-state database, excluding AS External LSAs.
- **Area LSA Chksum Sum**—32-bit unsigned sum of the link-state advertisements' LS checksums contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link-state database and to compare the link-state database of two routers.

- **Area SPF Run Count**—Number of times that the intra-area route table has been calculated using this area's LSDB.
- **ABR Count**—Number of ABRs reachable within this area.
- **ASBR Count**—Number of ASBRs reachable within this area.

Related Commands

[delete ospf default_area](#)

[disable ospf area](#)

[enable ospf area](#)

[set ospf area](#)

[set ospf default_area_id](#)

[show ospf area <area_id> settings](#)

show ospf global counters

This command displays current global OSPF counters.

Syntax

```
show ospf global counters
```

- **Router ID**—IP address of the router card.
- **External LSA Count**—Number of external (LS type 5) link-state advertisements in the link-state database since OSPF was enabled.
- **External LSA Checksum Sum**—A 32-bit unsigned sum of the LS checksums of the external link-state advertisements contained in the LSDB. This sum can be used to determine if the router's link state database has changed, and to compare the link-state database of two routers.
- **Originate New LSAs Count**—Number of new link-state advertisements that have been originated since OSPF was enabled. This number is incremented each time the router originates a new LSA.
- **Receive New LSAs Count**—Number of link-state advertisements received determined to be new instances. This number does not include newer instants of self-originated link-state advertisements.

Related Commands

[delete ospf default_area](#)

[disable ospf area](#)

[enable ospf area](#)

[set ospf area](#)

[set ospf default_area_id](#)

[show ospf area <area_id> settings](#)

Ping

This section covers Ping commands available using the CLI.

show ping row <row_number> counters

This command displays counters for the specified row in the Remote Ping Table. These settings reflect the configuration you specified using the [ping](#) command.

Status

```
show ping row <row_number> counters
```

- **Status**—The present state of this row. Possible states include 'notReady,' 'notInService,' and 'active.'
- **Count**—Number of pings to be transmitted in this sequence.
- **Requests Sent**—Number of pings sent when this row became active.
- **Replies Received**—Number of pings received when this row became active.
- **Timeouts Occurred**—Number of requests timed-out since this row became active.
- **Last Round Trip**—The round trip time in milliseconds experienced by the last request-reply iteration. A round trip value of **-1** indicates failed resolution.
- **Minimum Round Trip**—The minimum ping round trip time in milliseconds, not including timed out requests.
- **Maximum Round Trip**—The maximum ping round trip time in milliseconds, not including timed out requests.
- **Average Round Trip**—The average ping round trip time in milliseconds, not including timed out requests.
- **Creation Time**—When this row was created in terms of system up time.
- **Activation Time**—When this row was last activated in terms of system up time.
- **Last Changed Time**—When any object in this row was last changed in terms of system up time.

show ping server <host name or IP address> counters

This command displays ping server counters associated with the ping server specified with [add ping service loss system](#).



Average Time is expressed in milliseconds. Also, a value of -1 indicates the ping system failed.

Syntax

```
show ping server <host name or IP address> counters
```

Related Commands

[add ping service loss system](#)

PPPoE Commands

This section covers commands to show Point to Point Protocol over Ethernet (PPoE) counters.

show pppoe [counters | settings]

This command displays PPoE counter and settings information.

Syntax

```
show pppoe [counters | settings]
```

Counters displays PPPoE counters which are maintained for all control packets.

Settings displays the PPPoE configuration settings set by the set pppoe command.

PPTP Commands

This section covers commands to show Point to Point Tunnelling Protocol (PPTP) counters.

show pptp counters

This command displays statistics for configured PPTP tunnels.

Syntax

```
show pptp counters
```

- **Number of Active Tunnels**—Sum of currently active tunnels
- **Active Sessions**—Sum of currently active sessions
- **Malformed Packets**—Sum of packets containing structural errors
- **Control Tunnel Receive Packets**—Sum of control packets received since last initialized
- **Processed Control Tunnel Receive Packets**—Sum of received control packets processed with data by since last initialized

- **Control Tunnel Send Packets**—Sum of control packets transmitted since last initialized
- **Data Tunnel Receive Packets**—Sum of data packets received
- **Data Tunnel With Data Receive Packets**—Sum of data packets received with data
- **Data Tunnel Without Data Receive Packets**—(zero length bytes) dataless acknowledgement packets
- **Processed Data Tunnel Receive Packets**—Sum of received and processed data packets
- **In Sequence Data Tunnel Receive Packets**—Sum of data packets received in sequence
- **Out of Sequence Data Tunnel Receive Packets**—Sum of data packets received in out of sequence
- **In Order Data Tunnel Receive Packets**—Sum of data packets received in order
- **Out of Order Data Tunnel Receive Packets**—Sum of data packets received out of order
- **Flow Discarded Data Tunnel Receive Packets**—Sum of receive data packets dropped due to flow control
- **Out of Order Discarded Data Tunnel Receive Packets**—Sum of out of order receive data packets dropped
- **Data Tunnel Send Packets**—Sum of send data packets
- **Data Tunnel With Data Send Packets**—Sum of data packets sent containing data
- **Data Tunnel Without Data Send Packets**—Sum of data packets sent without data
- **Data Tunnel Flow Control Timeouts**—Sum of data channel flow control timeouts
- **Local Data Tunnel Flow Control Enables**—Sum of data channel flow control enables
- **Remote Data Tunnel Flow Control Enables**—Sum of remote data channel flow control enables
- **Data Tunnel Reassembly Timeouts**—Sum of data channel reassembly timeouts

RADIUS

This section covers commands to show Remote Authentication Dial-in User Service (RADIUS) counters.

show radius resource_management counters

This command displays RADIUS resource management counters on a per-server basis.

Syntax

```
show radius resource_management counters
```

- Resource Management Counters Start Time
- Queries received from Primary Server
- Query Responses sent to Primary Server
- Reclaims received from Primary Server
- Successful Frees sent to Primary Server
- Retransmitted Frees to Primary Server
- Queries received from Secondary Server
- Query Responses sent to Secondary Server
- Reclaims received from Secondary Server
- Successful Frees sent to Secondary Server
- Retransmitted Frees to Secondary Server
- Queries received from Tertiary Server
- Query Responses sent to Tertiary Server
- Reclaims received from Tertiary Server
- Successful Frees sent to Tertiary Server
- Retransmitted Frees to Tertiary Server

Related Commands

[disable radius resource_management](#)

[enable radius resource_management](#)

[show radius resource_management_settings](#)

RSH Process Commands

This section covers commands to show remote shell counter information.

show rshd counters This command show the current values of the system counters for the rsh process.

Syntax

```
show rshd counters
```

SNMP Commands

This section covers Simple Network Management Protocol (SNMP) commands in the CLI.

show snmp counters This command displays many SNMP input and output statistics.

Syntax

```
show snmp counters
```

Input Counters

- **Packets**—Number of SNMP packets received
- **Bad Versions**—SNMP messages for an unsupported SNMP version
- **Bad Community Names**—SNMP messages which used an unknown SNMP community name
- **Bad Community Uses**—SNMP messages which represented an SNMP operation not allowed by the SNMP community named in the message
- **ASN.1 Parse Errors**—Sum of ASN.1 or BER errors
- **Too Big Errors**—SNMP PDUs for which the value of the error-status field is 'tooBig'
- **No Such Name Errors**—SNMP PDUs where error-status field is 'noSuchName'
- **Bad Value Errors**—SNMP PDUs where error-status field is 'badValue'
- **Read Only Errors**—SNMP PDUs where the error-status field is 'readOnly'
- **General Errors**—SNMP PDUs where the error-status field is 'genErr'
- **Total Request MIB Objects**—Sum of MIB objects retrieved successfully as the result of receiving valid SNMP Get-Request and Get-Next PDUs
- **Total Set MIB Objects**—Sum of MIB objects altered successfully as the result of receiving valid SNMP Set-Request PDUs
- **Get Request PDUs**—Sum of SNMP Get-Request PDUs accepted and processed
- **Get Next Request PDUs**—Sum of SNMP Get-Next PDUs accepted and processed

- **Set Request PDUs**—Sum of SNMP Get-Next PDUs accepted and processed
- **Get Response PDUs**—Sum of SNMP Get-Response PDUs accepted and processed
- **Trap PDUs**—Sum of SNMP Trap PDUs accepted and processed

Output Counters

- **Packets**—Sum of SNMP packets transmitted
- **Too Big Errors**—Sum of SNMP PDUs generated by SNMP and for which the value of the error-status field is `tooBig`
- **No Such Name Errors**—Sum of SNMP PDUs generated by SNMP and for which the value of the error-status field is `noSuchName`
- **Bad Value Errors**—Sum of SNMP PDUs generated by SNMP and for which the value of the error-status field is `badValue`
- **General Errors**—Sum of SNMP PDUs generated by SNMP and for which the value of the error-status field is `genErr`
- **Get Request PDUs**—Sum of SNMP Get-Request PDUs sent from SNMP
- **Get Next Request PDUs**—Sum of SNMP Get-Next PDUs sent from SNMP
- **Set Request PDUs**—Sum of SNMP Set-Request PDUs sent from SNMP
- **Get Response PDUs**—Sum of SNMP Get-Response PDUs from SNMP
- **Trap PDUs**—Sum of SNMP Trap PDUs sent from SNMP

Tunnel Switch (L2TP & PPTP)

This section covers commands to perform tunnel switching functions using the CLI.

show tunnel switch_counters

This command displays switch statistics for L2TP and PPTP tunnels including the sum of total or current L2TP tunnels switched to PPTP tunnels and vice versa.

Syntax

```
show tunnel switch_counters
```

TFTP

This sections covers commands for using Trivial File Transfer Protocol (TFTP) functions in CLI.

show tftp request This command displays statistics of the specified request for TFTP service.

Syntax

```
show tftp request <input_file_name>
```

- **Filename**—Name of file to be requested from or sent to the TFTP server.
- **Server**—Name or IP address of the TFTP server.
- **Action**—Type of request send to the TFTP server. PUT or GET
- **Mode**—The text format the file is transmitted as. Choices: ASCII or OCTET (binary). The default is ASCII.
- **Retransmit Timeout**—Interval in seconds the router card waits for a reply from the TFTP server before retransmitting a TFTP request. The range is 1 to 60. The default is 5 seconds.
- **Maximum Timeout**—Interval in seconds the router card waits for a response from the TFTP server before the TFTP request is cancelled. The range is 1 to 300. The default is 25 seconds.
- **Status**—State of each current TFTP request in the table:
 - **Normal**—Request is in the table or has been successfully completed
 - **Getting**—Initial state: TFTP server is receiving a file
 - **Putting**—Initial state: TFTP server is sending a file
 - **Error**—Request has finished unsuccessfully and generates an error message
- **Error String**—Error message detailing why TFTP request has failed.

list tftp requests This command displays statistics of all current requests for service in the TFTP Client Request Table.

Syntax

```
list tftp requests
```

- **Filename**—Name of file to be requested from or sent to the TFTP server
- **Server**—Name or IP address of the TFTP server
- **Action**—Type of request send to the TFTP server. Put or Get
- **Status**—State of each current TFTP request in the table:
 - **Normal**—Request is in the table or has been successfully completed

- **Getting**—Initial state: TFTP server is receiving a file
- **Putting**—Initial state: TFTP server is sending a file
- **Error**—Request has finished unsuccessfully and generates an error message

Related Commands

[add tftp request](#)

[disable tftp request](#)

[enable tftp request](#)

Packet Bus Datagrams

This section covers commands to list packet bus datagram information using the CLI.

list pbus datagrams

This command displays statistics associated with packet bus datagrams (currently zero since the datalink driver doesn't support UI frames). It also shows the hardware setting for the pbus clock. When the Clock Statistic is *master*, the router card provides clocking. When the Clock Statistic is *slave*, another card provides the clock. When the Error Statistic displays 1, the pbus is operating normally.



In systems with clock backplanes, no master is designated. All new backplanes are clocked.

Syntax

```
list pbus datagrams
```

Traceroute

traceroute

This command displays the route (each hop) that a data packet takes from its source to a specified destination on the network and the time in milliseconds to reach each hop and return, generating all information received up to resolution or failure. Traceroute utilizes ICMP to monitor network messages and UDP to send out the packet. The command also can be implemented from an SNMP station. Router DNS services are always used to resolve names and/or verify addresses in dot notation. An address of zero indicates there was no response from that hop.



A row times out after 30 minutes and automatically is deleted. Also, a row can be deleted at any time, regardless of its state of status.

Be aware that traceroute-generated packets received by the router card will not increment ICMP error counters (Time Exceeded and Destination Unreachable).

Syntax

```
traceroute <IP name or address>
  maxhops <number>
  port <UDP port>
  retries <retries per hop>
  size <data size>
  timeout <timeout per hop>
```

Error messages are generated for the following reasons:

- **DNS Failed**—Destination address could not be resolved due to timeout or other reason
- **Bad address**—Resolved IP address is illegal
- **Hop Timeout**—Timeout occurred
- **Hops Exceeded**—Maximum number of hops exceeded
- **Dest(ination) Unreachable**—A route to the host could not be found
- **Tracing**—Performing traceroute
- **Resource Failure**—Not enough resources to complete the command

Related Commands

[set traceroute maximum_rows](#)

[show traceroute row <number> settings](#)

[list traceroute](#)

[delete traceroute row](#)

list traceroute This command displays the current rows in the main traceroute table when entered from an SNMP station or via a command file. Rows entered from the CLI are automatically deleted upon traceroute completion but rows entered from an SNMP station persists for 30 minutes.

Syntax

```
list traceroute
```

- **Row**—Rows currently active in Traceroute Table
- **Destination**—Host name or IP address of traceroute target
- **Hop Count**—Number of hops traceroute has traveled to reach destination
- **State**—Status of traceroute process associated with this row

When using SNMP or a command file only to perform a traceroute list, the following states may be reported.



Traceroute-generated packets received by the router card will not increment the ICMP error counters Time Exceeded and Destination Unreachable. See attributes below.

- **Active**—Specified IP address (host) is resolve
- **Not Active**—Before this row is activated
- **Waiting DNS**—Awaiting DNS resolution
- **DNS Failed**—Destination address could not be resolved due to timeout or other reason
- **Bad address**—Resolved IP address is illegal
- **Hop Timeout**—Timeout occurred
- **Hops Exceeded**—Maximum number of hops exceeded
- **Dest Unreachable**—A route to the host could not be found
- **Tracing**—Performing traceroute
- **Completed**—Traceroute completed successfully
- **Resource Failure**—Not enough resources to complete the command

Related Commands

[traceroute](#)

[delete traceroute row](#)

[set traceroute maximum_rows](#)

[show traceroute settings](#)

**list traceroute row
<number> hops**

This command displays counters for specified traceroutes.

Syntax

```
list traceroute row <number> hops
```

- **Row**—Entry number in the Traceroute Table. The range is 1 to 255.
- **Hop**—Number of hops taken to reach destination
- **IP address**—IP address of destination
- **Round Trip Time**—Period to reach destination and return to the router card

delete traceroute row

This command removes a specified row from the main traceroute table when entered from an SNMP station or via a command file. The CLI deletes the row immediately upon completion of the traceroute. The range is 1 to 65535.

Syntax

```
delete traceroute row <number>
```

Related Commands

[traceroute](#)

[list traceroute](#)

[set traceroute maximum_rows](#)

[show traceroute settings](#)

**set traceroute
maximum_rows**

This command sets a ceiling of traceroute entries in the Traceroute Table. Setting this value to a number smaller than the current number of rows will NOT cause any row deletions—but, the effect will be noted in future attempts at row creation. The range is 1 to 255. The default is 20.

Syntax

```
set traceroute maximum_rows <number>
```

Related Commands

[list traceroute](#)

[delete traceroute row](#)

[show traceroute settings](#)

show traceroute settings This command displays the maximum number of traceroutes configurable using the `set traceroute maximum_rows` command.

Syntax

```
show traceroute settings
```

Related Commands

[traceroute](#)

[list traceroute](#)

[delete traceroute row](#)

[set traceroute maximum_rows](#)

show traceroute row <number> settings This command displays results of the specified trace (entry in the Traceroute Table) using the [traceroute](#) command.

Syntax

```
show traceroute row <number> settings
```

- **State**—Status of the specified traceroute in the table. Possible states:
 - **WAITING DNS**—Waiting for DNS resolution
 - **DNS FAILED**—Destination address could not be resolved
 - **Bad address**—Resolved IP address is illegal
 - **HOPS EXCEEDED**—Maximum number of hops was exceeded
 - **DEST UNREACHABLE**—Trace timed out because route to the host could not be found
 - **TRACING**—Performing traceroute
 - **COMPLETED SUCCESSFULLY**—Traceroute completed successfully
 - **RESOURCE FAILURE**—Not enough resources to complete the command
- **Hop Timeout**—Interval in seconds before the router card retries a hop. The default is 3.
- **Hop Probes**—Maximum attempts the router card makes to learn a hop before moving to the next hop. The default is 3.
- **Max Hops**—Maximum number of hops the router card takes to trace before quitting. The default is 30.
- **UDP Port**—The router card port number used trying to find the route. The default is 33434.
- **Data Size**—Amount of data in bytes sent in the traceroute packet. The range is 1-8184 bytes.

- **Hop Count**—Number of hops the router card takes to reach the destination.

Telnet Commands

Telnet commands are available to users who dial in, whose *type* is network (type parameter in add user command), whose *host type* is prompt (host_type parameter in set login user command), and whose *login service* is Telnet (login_service parameter in set login user command).

telnet This command establishes a Telnet client session with the specified IP host name or address. In order for the system to resolve the host name, you must either add the host name and address to the DNS Local Host Table, or define a DNS server.

Syntax

```
telnet <IP name or address>
```

telnet <IP_name or address> TCP_port <number> This command establishes a Telnet client session with the specified IP host name or address using the specified TCP port number. It works just like the Telnet command, except you also specify the TCP port number to be used. The default TCP port number is 23. The maximum is 65535.

Syntax

```
telnet <IP_name or address> TCP_port <number>
```

Related Commands

[add user](#)

[set login user](#)

Dial-in User Telnet Commands

Telnet commands are available to users who dial in, and whose *type* is login (the *type* parameter in the add user command), and whose *host type* is prompt (the *host_type* parameter in the set login user command).

connect This command links a dial-in user to the specified IP host using a default login service and port number. After connecting, the user is prompted for a login and password to the host.

Syntax

```
connect <IP name or address>
```

exit This command leaves the CLI but keeps the connection open. This command returns you to Dial-In user or Telnet commands.

Syntax

```
exit
```

help This command displays the available Dial-in user commands.

Syntax

```
help
```

logout This command leaves the CLI and closes the connection. This ends the dial-in user's or Telnet session.

Syntax

```
logout
```

manage This is only shown if your user type is defined as *manage*. It allows you to execute full CLI commands and configure the system.

Syntax

```
manage
```

Related Commands

[CLI Exit Commands](#)

rlogin This command establishes an rlogin client session with the specified IP host name or IP address and TCP port number (optional). You must have run `add DNS host` or `add DNS server` for the system to recognize an IP host name. The default TCP port number is 513.

Syntax

```
rlogin <IP name or address>
      TCP_port <number>
```

telnet Establishes a Telnet connection to the specified IP address or host name. You must have run `add DNS host` or `add DNS server` for the system to recognize an IP host name. The default port number is 23.

Syntax

```
telnet <IP name or address> tcp_port <number>
```



You should run RIP when setting up a global IP network if you intend to support TCP services such as Telnet, rlogin and ClearTCP. Without RIP on the internal network, you won't learn of remote networks should the Ethernet interface be disabled.

set telnet admin_banner_file This command creates a banner file that is displayed when a successful telnet session is established.

Syntax

```
set telnet admin_banner_file <string>
```

Telnet Commands (Console Port)

The following commands are available to Console port users who Telnet from the Console port. Such users can access these commands by using the Telnet escape command: **Ctrl]** (right bracket). This function is not supported for login users.

close This command ends the active Telnet connection.

Syntax

```
close
```

help This command describes the available commands.

Syntax

```
help
```

send This command transmits a Telnet control character.

Syntax

```
send <string>
```

The available commands are:

Table 21 Send Command Parameter Descriptions

Parameters	Description
AYT	Are you there
IP	Interrupt process
BRK	Break
AO	Abort output
EC	Erase character
EL	Erase link
GA	Go ahead
NOP	No operation
EOR	End of record
SYNC	Synchronize
ESC	Escape

set escape This command allows changing the Telnet escape character from Ctrl] (right bracket] to something else. Control characters are specified using the caret character followed by the character.

Syntax

```
set escape <string>
```

Example

To set the Telnet escape character to *Ctrl x*, enter:

```
set escape ^ x
```

status This command displays the IP address of the remote host you are telneted to and the value of the Telnet escape character.

Syntax

```
status
```

Other Telnet Related Commands

This section covers additional or advanced Telnet commands available through the CLI.

add telnet client

This command adds a Telnet client to the Telnet client access list. The enable telnet client_access command enables the use of the Telnet client access list. If the Telnet client access list is disabled, there is universal entry to the access router card by Telnet users.

By specifying a netmask, you can add network and subnetwork addresses. If no netmask is specified, the host netmask value is assumed. An IP address of 0.0.0.0 allows universal entry to the router card by Telnet users. See the delete telnet client command for more information. Also, issue the list telnet client command for a list of configured users. The default is Disabled.

Syntax

```
add telnet client <IP address/mask>
```

delete telnet client

This command removes a Telnet client from a table of users permitted to access the router card. You may also disable Telnet access globally with the disable telnet client_access command. See the add telnet client command for more information. Also, issue the list telnet client command for a list of configured users. The default is disabled.

Syntax

```
delete telnet client <IP_address/mask>
```

disable telnet disconnect_message

When disabled, the router card will not send *connection closed by foreign host* and similar messages when the connection is closed. The default is enabled.

Syntax

```
disable telnet disconnect_message
```

enable telnet disconnect_message

This command re-enables the telnet disconnect message.

Syntax

```
enable telnet disconnect_message
```

enable telnet This command allow various Telnet functions.

Syntax

```
enable telnet
    client_access
    disconnect_message
    escape
    terminal_download_mode
    trying_message
```

Table 22 Enable Telnet Command Parameter Descriptions

Parameter	Description
client_access	Allows users to Telnet into the router card based on the Telnet client access list. This command is used in conjunction with the add telnet client command. See the list telnet client command for settings. The default is Disabled.
disconnect_message	When enabled, it sends connection closed by foreign host and similar messages when the connection is closed. The default is enabled.
escape	All Telnet clients are permitted to use the escape character during a session. By default the escape character is Ctrl] (right bracket). A user can change that value using <code>set_escape</code> in the Telnet program.
terminal_download_mode	Turns off local and remote echo for Telnet on a TCP port other than 23 for a router card Telnet client. When enabled, this function forces Telnet clients to negotiate Telnet ECHO DISABLE for both local and remote sides of the connection. The default is Disabled.
trying_message	Turns on the trying status message for clients attempting to Telnet out of the router card. When escape is enabled, Telnet clients who issue the escape character during their session will get a local Telnet command line. This function is not supported for login users.

Related Commands

```
disable telnet
show time
```

disable telnet This command prevents various Telnet client services.

Syntax

```
disable telnet
    client_access
    escape
    terminal_download_mode
    trying_message
```

Table 23 Disable Telnet Command Parameter Descriptions

Parameter	Description
client_access	if client access is disabled, there is universal access to the router card from Telnet clients. The default is Disabled.
escape	All Telnet clients are prevented from using the escape character during a session.
terminal_download_mode	Disables feature which <i>turns off</i> local and remote echo for Telnet on a TCP port other than 23 for a router card Telnet client. The default is Disabled.
trying_message	Turns off the trying status message for clients attempting to Telnet out of the router card. When escape is disabled, Telnet clients who issue the escape character during their session will not get a local Telnet command line (the character is sent as regular text).

Related Commands

```
enable telnet
```

```
show time
```

list telnet clients

This command displays a list of Telnet clients you configured using the add telnet client command. When access is globally enabled with the enable telnet client_access command—capable of accessing the router card. By specifying a netmask, you can add network and subnetwork addresses. If no netmask is specified, the host netmask value is assumed. An IP address of 0.0.0.0 allows universal entry to the router card by Telnet users. See the delete telnet client command for more information. Also, issue the list telnet client command for a list of configured users. The default is disabled.

Syntax

```
list telnet clients
```

show telnet settings

This command displays the status of the Telnet escape and trying message features. It is set using the disable/enable telnet escape and trying_message commands.

Syntax

```
show telnet settings
```

Related Commands

[delete telnet client](#)

[enable telnet](#)

User Commands

You configure all remote networking parameters within the profile of the user who is dialing in. A user profile specifies the user's protocol, address parameters, and other unique settings.

add user This command adds a user to the Local User Table. You may specify a type for the user, as well as login and network protocols, or use the defaults.



Administrators creating RADIUS users should consult the Total Control 1000 Enhanced Data System Operations Guide for more information.

Syntax

```
add user <name>
    enabled [yes | no]
    login_service [rlogin | telnet | cleartcp | ping]
    network_service [ppp | slip]
    password <password>
    type [login, network, callback, dialout, manage]
```

Table 24 Add User Command Parameter Descriptions

Parameter	Description
[name]	Name of user to be added, up to 64 ASCII characters. The limit is no more than 451 local users.
enabled	<i>Optional.</i> Indicates whether the user is enabled (YES) or disabled (NO) by this command.
login_service	<ul style="list-style-type: none"> ■ Protocol to be used for a login user. Options are: ■ RLOGIN ■ TELNET (<i>default</i>) ■ ClearTCP ■ Ping—user pings a login host, receives a successful/unsuccessful message and is disconnected.
network_service	Framed protocol to be used by network user. Options: <ul style="list-style-type: none"> ■ PPP—Point-to-Point Protocol (<i>default</i>) ■ SLIP—Serial Line IP. SLIP is not supported currently for LAN-to-LAN users.
password	User password (optional). The limit is 127 ASCII characters. You can create a null password with: <i>password ""</i> .
type	Type of user—may be one or more types. <ul style="list-style-type: none"> ■ Login uses the login_service specified. ■ Network (<i>default</i>) uses network_service specified—a dial-in user. ■ Callback users are disconnected after authentication and called back. ■ Dialout—modem sharing or WAN users. ■ Manage users have administrative authority.

Related Commands

[delete user](#)
[disable user](#)
[disconnect user](#)
[enable user](#)
[list users](#)
[set user](#)
[show all users](#)
[show user](#)

delete user This command deletes a user you previously added to the Local User Table. Use [list users](#) to see the currently defined user.

Syntax

```
delete user <name>
```

Related Commands

[add user](#)
[disable user](#)
[enable user](#)
[show user](#)

disable user This command disables the specified user from being used. This affects dial-in users, and WAN connections that depend on that user for parameters. It also causes all active sessions established using that particular user to terminate, and does not allow any new sessions to occur using that user name. Disabling a user is useful when prohibiting a user's access temporarily. Use the [list users](#) and [show user](#) commands to view edits.

Syntax

```
disable user <user name>
```

Related Commands

[list users](#)
[show user](#)
[add user](#)
[delete user](#)
[enable user](#)

disconnect user This command brings down the specified user connection.

Syntax

```
disconnect user <name>
```

Related Commands

[add user](#)

[delete user](#)

[disable user](#)

[enable user](#)

[list users](#)

[set user](#)

[show all users](#)

[show user](#)

enable user This command allows a user to establish dial in and/or dial out sessions. Use [add user](#) to add a user. Use [list users](#) to see the current state of all users.

Syntax

```
enable user <name>
```

Related Commands

[list users](#)

[add user](#)

[delete user](#)

[disable user](#)

[show user](#)

list users This command displays all users and attributes you specified using the add and set user commands.

Syntax

```
list users
```

- **User Name**—User designation you specified using the add user command.
- **Login Service**—*TELNET*, *RLOGIN*, or *ClearTCP*
- **Network Service**—Type of network service. PPP or SLIP. SLIP service not supported for LAN-to-LAN users.
- **Status**—Link status. ACTIVE (in use), INACTIVE (not in use) or DISABLED (inactivated).
- **Type**—Type of configured user. See the [add user](#) command for more information.

Related Commands

[delete user](#)

[disable user](#)

[enable user](#)

[show user](#)

Set User Commands Set user commands allow you to change the configuration of the following user profiles.

set user This command configures a user and profile.

Set a secure password for users with administrative privileges. This command can also assign the default administrator "adm" a password.

Syntax

```
set user <user name>
    alternate_phone_number <number>
    callback_type [ani | dynamic | normal | static]
    chat_script_name <name>
    dnis_reauthentication [no_reauth | reauth_any | reauth_chap |
    reauth_eap | reauth_mschap | reauth_pap | reauth_proxy_eap]
    expiration <date>
    idle_timeout <interval>
    input_filter <filter_name>
```

```

message <string>
modem_group <group_name>
output_filter <filter_name>
password <password>
phone_number <number>
policy_access [disabled | enabled]
policy_configuration [dynamic | static]
policy_file <string>
policy_type [domain_based | user_based]
port_limit <number>
session_timeout <seconds>
special_xon_xoff_flow [disabled | enabled]
telnet_options [binary, escape]
traffic_threshold <0-99999>
type [login, network, callback, dialout, manage]

```



*If a filter file is specified without an extension, the router card assumes RADIUS input filter files have the extension **.in** and that RADIUS output filter files have the extension **.out**. For this reason, RADIUS filter files should be named **filter.in** and **filter.out**.*

Set user commands allow you to change the configuration of user profile settings, some of which may have already been configured by the add user command.

Table 25 Set User Command Parameter Descriptions

Parameter	Description
<user_name>	Name of user, previously defined using add user. The limit is 64 ASCII characters.
alternate_phone_number	Number to dial if the first number is busy. The limit is 33 ASCII characters. Note: This value is overridden when a dial-out script specified in the set dialout user command is issued.
callback_type	ani—Callback is initiated to the phone number identified in the caller ID information dynamic—Callback is initiated to a number (or 2 numbers separated by '&') negotiated through PPP. normal—Callback is initiated to the phone_number or alternate_phone_number stored in the user record. static—Callback is initiated to a phone number specified in a phone number pool.
chat_script_name	Designation of the Chat Script associated with this user. See add chat_script command for more.

Table 25 Set User Command Parameter Descriptions (continued)

Parameter	Description
dnis_reauthentication	<p>If the PPP authentication is configured for a re-authenticated user, then PPP tries to negotiate the specified protocol for PPP authentication.</p> <p>no_reauth—Do not reauthorize the user.</p> <p>reauth_any—Use any protocol to reauthorize the user.</p> <p>reauth_chap—Use CHAP to reauthorize the user.</p> <p>reauth_eap—Use EAP to reauthorize the user.</p> <p>reauth_mschap—Use MSCHAP to reauthorize the user.</p> <p>reauth_pap—Use PAP to reauthorize the user.</p> <p>reauth_proxy_eap—proxy EAP to reauthorize the user.</p>
expiration	<p>Date after which this user becomes inactive. The format is DD-<i>MMM</i>-[<i>YY</i>]<i>YY</i>. Month is the first 3 letters of the month. Year is either 2 or 4 digits—96 or 1996.</p>
idle_timeout	<p>Interval to wait before timing out an inactive connection. The default is 0 (not activated). The range is 1 to 86400 seconds.</p> <p>Note: Change the default to configure this value.</p>
input_filter	<p>Designation of the filter file in Flash memory to be applied to the input datastream.</p>
message	<p>String to display to a dial-in user when connection is set. The limit is 64 ASCII characters</p> <p>You can use \$value to stipulate more parameters in the message line for identification purposes.</p> <ul style="list-style-type: none"> ■ \$date—current date according to system uptime ■ \$callid—user’s call identification according to system uptime ■ \$port—port occupied by user (slot:x/mod:y) ■ \$hostname—user’s host name ■ \$sysname—user’s system name (same as hostname) ■ \$time—time of call according to system uptime <p>Note: The message, if it includes spaces, must be enclosed in quotations. Use the show user command to view the message as configured.</p>
modem_group	<p>Name of modem group used to make connection to this <i>dial-out</i> user.</p> <p>Important: This value does not apply to a dial-in user.</p>
output_filter	<p>Name of the filter file in Flash memory to be applied to the output datastream.</p>
password	<p>User’s password (optional). The limit is 127 ASCII characters. You may enter a null password with: <i>password ""</i>.</p>
phone_number	<p>Primary phone number to make the connection. The limit is 33 ASCII characters.</p> <p>Note: This value is overridden when a dial-out script specified in the set dialout user command is issued.</p>
policy_access	<p>This command is used to specify the interface (dial-up) type is public or private. This information is used by Policy and Flow Manager in determining the type of connections.</p>
policy_configuration	<p>Set the policy to either dynamic or static.</p>

Table 25 Set User Command Parameter Descriptions (continued)

Parameter	Description
policy_file	The name of the IPsec policy file in the system cache that is associated with this user account.
policy_type	Set the policy type to either domain-based or user-based.
port_limit	The maximum number of dial-in ports a local user can concurrently employ. This setting <i>does not apply</i> to Telnet users logged in through the Ethernet interfaces nor to remote users (RADIUS authenticated) who are assigned this value by the associated RADIUS server. The range is 1-475.
session_timeout	Interval before timing out a session. The default is 0 (no setting).
special_xon_xoff_flow	This parameter enables and disables the use of Xon/Xoff flow control for users that dial into the router card from a terminal that uses Xon/Xoff flow control. The default is disabled.
telnet_options	binary—Enables binary transfers during telnet sessions. escape—Enables escape sequences during telnet sessions. Entering this parameter with no a value disables that function. For example; the command set user <username> telnet_option binary escape enables both the binary and escape telnet options. The command set user <username> telnet_option escape disables the binary telnet option but leaves the escape option enabled.
type	Type of user added. A user may be one or more types but callback and dialout are mutually exclusive. <ul style="list-style-type: none"> ■ Login users are TCP users who use the login_service specified. ■ Network users are framed protocol users, who use the network_service specified. ■ Callback users disconnected after authentication and called back. ■ Dialout users are either modem sharing users or WAN connection users. ■ Manage users with system administration authority.

set dialout user

This command sets parameters for dial-out users, both WAN and modem. Send scripts are useful under the following conditions:

- **Dial-out sites**—User dials out to a remote location and is connected or prompted for a login.
- **Dial-in/dial-out**—User dials in to the router card, then dials out to a remote site and is connected.
- **Telnet/dial-out**—User telnets into the router card then dials out to a remote site and is connected as a *shared_modem* user.

Script strings are limited to 240 characters which must be enclosed in double quotes if exceeding 64 ASCII characters.



These values override phone or alternate phone numbers specified in the set user command.

Syntax

```

set dialout user <user name>
    local_IP_address <IP network address>
    reply1_script <"string">
    reply2_script <"string">
    reply3_script <"string">
    reply4_script <"string">
    reply5_script <"string">
    reply6_script <"string">
    send1_script <"string">
    send2_script <"string">
    send3_script <"string">
    send4_script <"string">
    send5_script <"string">
    send6_script <"string">

```

Table 26 Set Dialout User Command Parameter Descriptions

Parameter	Description
<user_name>	Name of user, previously defined using <i>add user</i> command with dialout as the type. The limit is 64 ASCII characters.
local_IP_address	IP address of the user making an IP connection over this dial-out interface.
send & reply scripts	Specify commands required to establish and terminate the remote connection. Scripts must be enclosed in double quotes if more than 64 ASCII characters. The limit is 240 ASCII characters.

set dialout user <user name> site

This command sets parameters for dial-out users connecting to a remote network.

Syntax

```

set dialout user <user name> site
    address_selection [assign | negotiate | specified]
    default_route_option [enable | disable]
    end_time <time>
    ip [enable | disable]
    ipx [enable | disable]
    ipx_address <IPX_address>
    remote_ip_address <IP_name or network address/mask_specifier>
    send_password <string>

```

```

spoofing [enable | disable]
start_time <time>
type [ondemand | timed | continuous | manual]

```

Table 27 Set Dialout User site Command Parameter Descriptions

Parameter	Description
address_selection	Determines how the IP address will be assigned for incoming (client) IP network connections. <ul style="list-style-type: none"> ■ Negotiate—brokers IP address between remote client and local user. ■ Assign—chooses address from IP pool, configured using <i>set ip system</i>. Default ■ Specified—<i>must</i> use IP address set in <i>remote_IP_address</i> value.
default_route_option	Automatically sets the IP address of a remote default router by <i>negotiation</i> . This parameter takes precedence over a default route (gateway) set by <i>add framed_route user</i> or <i>add ip defaultroute</i> commands, which require <i>manual</i> IP address entry. The default is Disable.
end_time	For a timed user, specifies when to tear down connection. Seconds field is optional.
ip	Determines if this connection supports IP or not. The default is Enable.
ipx	Determines whether this connection supports IPX or not.
ipx_address	The address of the remote network.
remote_IP_address/ mask_specifier	For a remote IP connection, the IP network address assigned to the client, in the format <i>nnn.nnn.nnn.nnn</i> , with or without a mask specifier. The mask specifier can be in IP address format (<i>255.0.0.0</i> or greater and contiguous) or 'A', 'B', 'C', or a numeric value from 8 to 30 that describes the number of one bits in the mask. If setting a user's IP address, the mask specifier is set to 'H' (for Host) or a numeric value of 32. If you don't specify a mask, the system generates it for you from the network address. The default is 0.0.0.0/H.
send_password	Password sent to remote network. Note: Passwords you define with other commands are for dial-in users. The limit is 63 ASCII characters.
spoofing	Specifies spoofing across the remote connection, to save overhead on the dial-out line's connection. The default is Disable.
start_time	Period to start a TIMED connection. Seconds field is optional.
type	Describes what type of dial out connection this is: <ul style="list-style-type: none"> ■ Ondemand—makes connection when the system seeks a session with the remote network. ■ Timed—makes connection at a set time ■ Continuous—always keeps connection up ■ manual—starts connection manually with CLI Default

set framed_route user This command specifies a framed (static) network to the user profile for dialup connections.

Syntax

```
set framed_route user <name>
    gateway <IP address>
    ip_route <IP address>
    metric <number>
```

Table 28 Set Framed_Route User Command Parameter Descriptions

Parameter	Description
<user name>	User name specified for the framed network.
gateway	IP address of the gateway used to reach this remote network.
ip_route	IP address of the remote network
metric	Integer representing how far away the route is, in “hops” from other routers. The range is 1 to 15.

Related Commands

[add framed_route user](#)
[delete framed_route user](#)
[add framed_route user](#)
[add ip route](#)

set login user This command sets parameters for users whose type is LOGIN.

Syntax

```
set login user <user name>
    host_type [prompt | select | specified]
    keep_alive_interval <0 to 65535>
    login_host_ip_address <IP name or address>
    login_host_name <IP name or address>
    login_service [rlogin | telnet | cleartcp | ping]
    tcp_port <number>
    terminal_type <string>
```

Table 29 Set Login User Command Parameter Descriptions

Parameter	Description
<user name>	User to set parameters for, earlier defined using add user with login as type. The limit is 64 ASCII characters.
host_type	Options are: <ul style="list-style-type: none"> ■ Prompt—Dial-in user is prompted to enter an IP host or address. ■ Select—User is connected to a host, which is chosen from the list of login hosts you defined using add login_host. The method of selecting the host is set using the set connection command (RANDOM or ROUND ROBIN). Default ■ Specified—Dial-in user connects to the login host set by the <i>login_host_ip_address</i> of this command.
keep_alive_interval	Time limit for the user.
login_host_IP_address	IP address or host name of the remote host.
login_host_name	Designation of host to be resolved at time of connection.
login_service	Service used to login to the remote host. Choices: <ul style="list-style-type: none"> ■ RLogin ■ Telnet—<i>Default</i> ■ ClearTCP ■ Ping—user pings a login host, receives a successful/unsuccessful message and is disconnected.
tcp_port	TCP Port number the remote host expects this login to use. The limit is 65535.
terminal_type	Terminal type used for the remote connection, e.g. VT100. The limit is 64 ASCII characters.

show user This command displays the parameters defined for the specified user.

Syntax

```
show user <name>
    settings
    all_settings
```

- **settings**—Displays settings for the specified user with the exception of *disabled IP, IPX, Tap Status and Tunnel Type* parameters.
- **all_settings**—Displays *all* settings for the specified user.

Related Commands

[add user](#)
[delete user](#)
[disable user](#)
[enable user](#)
[list users](#)

set maximum_local_users This command configures the total number of users that can be created locally on the router card. Use the [show maximum local users](#) command to display settings. The maximum is 1000.

Syntax

```
set maximum_local_users <number>
```

Related Commands

[show maximum_local_users](#)

Network User Commands

This section covers commands to configure network users using the CLI.

set network user This command specifies parameters for IP users whose *type* is network.

Syntax

```
set network user <name>
    header_compression [none | tcpip]
    mtu <number>
    network_service [fr_1490 | ppp | slip]
    ppp_source_ip_filter [enabled | disabled]
    ppp periodic_chap_timeout <0 to 65535>
    send_password <user password>
    spoofing [enable | disable]
```

Table 30 Set Network User Command Parameter Descriptions

Parameter	Description
mtu	Largest data packet size (bytes) allowed. The default is 1514. The range is 64-8192.
network_service	Framed protocol to be used by network user. Options: <ul style="list-style-type: none"> ■ fr_1490 ■ PPP—Point-to-Point Protocol (<i>default</i>) ■ SLIP—Serial Line IP. SLIP is not supported currently for LAN-to-LAN users.
send_password	Password sent to the remote network. The limit is 15 ASCII characters.
spoofing	Spoofing across remote connect to save overhead on dial-out line. The default is disabled.

set network user <user name> igmp

This command specifies IGMP parameters for users whose *type* is network.

Syntax

```
set network user <user name> igmp
  max_response_time <1 to 10>
  multicast_forwarding [enabled | disabled]
  multicast_proxy [enabled | disabled]
  query_interval <5 to 65535>
  robustness <1 to 5>
  routing [enabled | disabled]
  version [1,2]
```

Table 31 Set Network User_Command Parameter Descriptions

Parameter	Description
max_response_time	The interval a host has to respond to the IGMP query. The default is 10. The range is 1-10 seconds.
multicast_forwarding	Multicast packets are forwarded when enabled. The default is Disabled.
multicast_proxy	Multicast addresses that are joined or learned on the specified interface are joined on the proxy interface that is configured with the set ip multicast proxy interface command. The default is disabled.
query_interval	The frequency at which IGMP Host-Query messages are sent on the specified interface. The default is 125. The range is 5-65535.
robustness	Tuning parameter for expected packet loss on a subnet. If packet loss on a subnet is expected to be high, robustness may be increased. The range is 1-5. The default is 2.
routing	Attempts to become the IGMP querier on this interface. The default is disabled.
version	The version of IGMP running on this interface. This object can be used to configure a router capable of running either version. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN. The default is 2.

set network user <name> ip This command specifies parameters for IP users whose *type* is network. Routing for network users is host-based, so the subnet specified by the *remote_ip_address* parameter is a 32-bit mask, supplied either by the administrator or automatically, by the router card.



Administrators creating RADIUS users should consult the Total Control 1000 Enhanced Data System Operations Guide for more information.



Negotiate address selection does not support SLIP. If using routing, you must turn it on since the default is none.

Syntax

```
set network user <name> ip
    address_selection [negotiate | assign]
    default_route_option [enable | disable]
    iea_next_hop_gateway <IP_name or network
address/mask_specifier>
    remote_ip_address <IP_name or network address/mask_specifier>
    rip_authentication_key <string>
    rip_policies_update <rip policies>
    routing [listen | send | both | none]
    routing_protocols
[ripv1,ripv2,ospf,no_ripv1,no_ripv2,no_ospf]
    usage [enable | disable]
```

Table 32 Set Network Command Parameter Descriptions

Parameter	Description
<user name>	User, who must have network as the type.
address_selection	Determines how IP address will be assigned for incoming (client) IP network connections. <ul style="list-style-type: none"> ■ Negotiate—brokers IP address between remote client and local user. Note: Negotiate is not available with SLIP. ■ Assign—chooses address from IP pool, configured using set ip system. Default.
default_route_option	Automatically sets the IP address of a remote default router by <i>negotiation</i> . This parameter takes precedence over a default route (gateway) set by add framed_route user or add ip defaultroute commands, which require <i>manual</i> IP address entry. The default is Disable.
iea_next_hop_gateway	Configures the IP address of an IEA next hop gateway. Also see enable ip iea_force_nexthop_routing and disable ip iea_force_nexthop_routing.

Table 32 Set Network Command Parameter Descriptions (continued)

Parameter	Description
remote_IP_address/mask_specifier	For a remote IP connection, the IP network address assigned to the client, in the format <i>nnn.nnn.nnn.nnn</i> , with or without a mask specifier. The mask specifier can be in IP address format (<i>255.0.0.0</i> or greater and contiguous) or 'A', 'B', 'C', or a numeric value from 8 to 30 that describes the number of one bits in the mask. If setting a user's IP address, the mask specifier can also be 'H' (for Host) or a numeric value of 32. If you don't specify a mask, the system generates it for you from the network address. The default is 0.0.0.0/H.
rip_authentication_key	Authorizes RIP updates using a stored password. Maximum string length: 64 ASCII characters.
rip_policies_update	Allows user to enable or disable RIP policies. See the set ip network <name> command for description of keywords. A keyword with a no_ in front is used to disable the policy. The default is indicated by (D). Note: For Poison Reverse to work properly, Split Horizon must also be enabled. SEND_DEFAULT NO_SEND_DEFAULT(D) SEND_ROUTES(D)NO_SEND_ROUTES SEND_SUBNETSNO_SEND_SUBNETS(D) ACCEPT_DEFAULTNO_ACCEPT_DEFAULT(D) SPLIT_HORIZON(D)NO_SPLIT_HORIZON POISON_REVERSENO_POISON_REVERSE(D) FLASH_UPDATE(D)NO_FLASH_UPDATE SEND_COMPAT(D)NO_RIPV1_SEND RIPV1_RECEIVE(D)NO_RIPV1_RECEIVE RIPV2_RECEIVE(D)NO_RIPV2_RECEIVE SILENT (default is disabled)
routing	Sets routing type (RIP packets) accepted on this connection. The choices: <ul style="list-style-type: none">■ Listen—detects packets destined for system's networks■ Send—routes packets destined for the remote network■ Both—both listens and sends■ None—ignores all routing packets. Default.
routing_protocols	Sets and unsets routing protocols for the IP user. To set a protocol, use the values <i>ripv1</i> , <i>ripv2</i> , or <i>ospf</i> . To unset a protocol, use the values <i>no_ripv1</i> , <i>no_ripv2</i> or <i>no_ospf</i> . Set and unset values can be used in the same command line. When specifying more than one value, put commas between the choices with no space after the comma. For example; set network user joesmith ip routing_protocols ripv1,ripv2,ospf. The default is <i>ripv1</i> .
usage	Sets interface to enable/disable IP protocol. The default is Enable.

set network user <user name> ipx

This command specifies IPX parameters for users whose *type* is set to *network*.

Syntax

```
set network user <user name> ipx
  address <ipx network address>
  rip_age_multiplier <interval>
  rip_update <interval>
  routing [all | listen | respond | send | none]
  sap_age_multiplier <interval>
  sap_update <interval>
  usage [enable | disable]
  wan [enable | disable]
```

Table 33 Set Network User Command Parameter Descriptions

Parameter	Description
address	IPX address of the remote network. When configuring for an unnumbered IPX network, set this value to <i>ffffffc</i> . The default is 00000000.
rip_age_multiplier	Sets holding multiplier for data received in RIP periodic updates. The default is 3.
rip_update	Sets interval, in seconds, between RIP periodic updates. The default is 60 seconds.
routing	Sets type of IPX RIP and SAP packets to accept on this connection. <ul style="list-style-type: none"> ■ Listen—detects RIP/SAP packets headed for system’s networks ■ Send—routes packets destined for remote network ■ Respond—if requested, responds with IPX RIP or SAP data. Default ■ All—Detects, sends, responds with RIP/SAP packets ■ None—ignores all routing packets
sap_age_multiplier	Sets holding multiplier for data received in SAP periodic updates. The default is 3.
sap_update	Sets interval, in seconds, between SAP periodic updates. The default is 60 seconds.
usage	Sets interface to enable/disable IPX protocol. The default is enabled.
wan	Protocol used between two IPX networks negotiating the IPX network number for a WAN connection. Both ends of the connection must enable this protocol for it to work. The default is disabled.

set network user <user name> ppp

This command sets parameters for users whose *type* is network, and who will connect over an interface running multilink PPP (MLPPP). Adding a network PPP user to the User Table *automatically* enables MLPPP, which serves to group multiple links into a bundle to combine the communications capacity of both links. This applies to ISDN service, where there are two bearer channels, and your provider allows combining both channels on demand.



Since default values for channel decrement and expansion are 0, to employ ondemand allocation, change the settings to suit your anticipated bandwidth traffic. CommWorks recommends settings of 20 (decrement) and 60 (expansion).



To ensure MLPPP is up on both ends of the connection, do not change the max_channels default value of 2 otherwise MLPPP may fail.

Syntax

```
set network user <user name> ppp
    channel_decrement <percent>
    channel_expansion <percent>
    compression_algorithm [ascend | auto | microsoft | none |
    stac]
    encryption_algorithm [auto | microsoft_128bit |
    microsoft_40bit | microsoft_56bit |
    none | required]
    expansion_algorithm [constant | linear]
    max_channels <number>
    min_size_compression <number>
    periodic_chap_timeout <seconds>
    primary_dns_server <IP DNS address>
    receive_acc_map <hex number>
    reset_mode_compression [auto | every_packet | every_error]
    secondary_dns_server <IP DNS address>
    transmit_acc_map <hex number>
```

Table 34 Set Network User PPP Command Parameter Descriptions

Parameter	Description
<user name>	Name user, previously defined using add user with network as the type.
channel_decrement	When line usage on the second channel drops below this percentage, PPP drops the second (QUAD) or more (HDM only) channels. The default is 0. Recommended: 20. The range is 1-100%.
channel_expansion	When the line usage of the first channel exceeds this percentage, PPP adds the second (QUAD) or more channels (HDM: up to 16). Specifying 100% disables the second and additional channels for multilink PPP. The default is 0. Recommended: 60. The range is 1-100%.
compression_algorithm	Specifies the proprietary compression algorithm PPP uses via negotiation. Choices are: ASCEND, MICROSOFT, STAC and NONE. The default is AUTO. Note: This value can be overridden by using the set ppp ccp_modemtype command. If you know the type of traffic your connection will bear, using this command is beneficial.
encryption_algorithm	Type of encryption algorithm to employ for this user. Choices: <ul style="list-style-type: none"> ■ None—no encryption used on this link. ■ Auto—attempt to negotiate all encryption algorithms is made, but if none are successful, the link remains up. ■ Microsoft_40bit—only 40-bit MPPE (Microsoft Point-to-Point Encryption) is used, if not available, the link fails. ■ Microsoft_56bit—only 56-bit MPPE (Microsoft Point-to-Point Encryption) is used, if not available, the link fails. ■ Microsoft_128bit—only 128-bit MPPE is used, if not available, the link fails. ■ Required—either 40-bit or 128-bit MPPE is used (128-bit first), if neither is available, the link fails.
expansion_algorithm	Specifies which type of expansion algorithm to handle bandwidth allocation. <ul style="list-style-type: none"> ■ CONSTANT—A long-term measurement and allocation of traffic bandwidth best for constant datastreams, such as file transfer. Default ■ LINEAR—A short-term measurement and allocation of traffic bandwidth, best for bursty traffic, such as interactive users.
max_channels	Sets how many channels to use for multi-link PPP (MLPP). This value either invokes PPP to negotiate for MLPPP with the remote system (more than 1) or does not try to negotiate for MLPPP (1). The actual number of channels used is determined by channel_decrement and expansion parameters. MLPPP is on by default with a value of 2. Note: To ensure that MLPPP is running on both ends of a connection, do not lower the default value of 2 otherwise MLPPP may fail. For HDM cards only, you may set up to 16 channels.
min_size_compression	Data packet size that PPP decides is big enough to start compression. Data packets smaller than that will not be compressed. The range is 0-2048 bytes. The default is 256.

set network user
<user_name>
ppp_source_ip_filter
[enabled | disabled]

This command configures the Return Route Assurance (RRA) feature used to guarantee that a dial-up user can not spoof or use someone else's source IP address. When RRA is enabled, the router card only routes client packets containing a source IP address consistent with the negotiated IP address (the router card discards all other packets). When this feature is disabled, the router card does not perform any special actions.

Syntax

```
set network user <user_name> ppp_source_ip_filter [enabled |
disabled]
```

The default is Disabled. The value *<user name>* is the name of a user previously defined by the add user command with type set to network.

Tunnel User Commands

set tunnel user

This command configures parameters for local users employing tunneling via L2TP, PPTP or other protocols. Authentication is performed using a Message Integrity Check (MIC) which is added to each packet generated from the shared secret (password or key). This key is renegotiated often between server/client peers. An additional degree of security is available for control, data or data and control packets.

Syntax

```
set tunnel user <user_name>
assignment_id <64 character string>
client_endpoint <string>
group <string>
medium_type <ipv4>
password <user_password>
security [none | control_only | data_only |
both_data_and_control]
server_endpoint <string>
type [none | pptp | l2tp]
```

Table 35 Set Tunnel User Command Parameter Descriptions

Parameter	Description
<user_name>	Name of the user, previously defined using the add user command. The limit is 64 ASCII characters.
assignment_id	64 ASCII character ID string
type	The tunneling protocol this user will employ. Choices: <ul style="list-style-type: none"> ■ none—No tunneling specified ■ pptp—Point-To-Point Tunneling Protocol—Microsoft’s tunneling protocol. Default ■ l2tp—Layer 2 Tunneling Protocol
medium_type	The transport layer of the tunnel medium used when creating tunnels. The only choice available is ipv4, which is the default.
client_endpoint	The IP address of the initiator-end of the tunnel. The limit is 64 ASCII characters.
server_endpoint	The IP address of the server-end of the tunnel. The limit is 64 ASCII characters.
password	The shared secret between tunnel server and client. The limit is 63 ASCII characters.
group	Group ID of the tunneled session. The limit is 64 ASCII characters.
security	Additional degree of security to perform on control or data packets for this tunnel. Choices: none, control-only, data-only, or both-data-and-control.

Address Pool User Commands

This section covers commands to add and delete address pool users through the CLI.

add address_pool user This command assigns a user to a previously configured address pool.

Syntax

```
add address_pool user <user_name>
    pool_name <name>
```



When creating an address pool user, be sure to verify that a valid address pool exists.

Related Commands

[add ip pool](#)
[delete address_pool user](#)
[disable ip address_pool_filtering](#)
[enable ip address_pool_filtering](#)
[set ip pool](#)

delete address_pool user This command removes a user which was previously assigned to the specified address pool via the add address_pool user command.

Syntax

```
delete address_pool user <name>
    pool_name <name>
```

Related Commands

[add address_pool user](#)

[add ip pool](#)

[enable ip address_pool_filtering](#)

[set ip pool](#)

Security Option Commands

disable security_option remote_user_administration This command disables CLI access by remote Telnet and dial-in users. All CLI configuration must be done from the console port.

Syntax

```
disable security_option remote_user_administration [dialin |
telnet]
```

Related Commands

[enable security_option remote_user_administration](#)

enable security_option remote_user_administration This command allows CLI access by remote Telnet (network) or dial-in users. CLI configuration can be done from the console port and by remote users.

Syntax

```
enable security_option remote_user_administration [dialin |
telnet]
```

Related Commands

[disable security_option remote_user_administration](#)

[enable security_option snmp_user_access](#)

TCP

disable tcp keepalives This command disallows TCP keep-alive support for all TCP sessions begun after this command is issued. The default is disabled.

Syntax

```
disable tcp keepalives
```

Related Commands

[enable tcp keepalives](#)

[show tcp](#)

disable tcp nagle_algorithm This command disallows use of the Nagle algorithm to allow transmission of small packets for TCP applications which require them. This algorithm withholds additional packet transmissions to an output buffer until there is sufficient data to fill a maximum-sized segment. The default is enabled.

Syntax

```
disable tcp nagle_algorithm
```

Related Commands

[enable tcp nagle_algorithm](#)

[show tcp](#)

enable tcp keepalives This command permits TCP keep-alive support for all TCP sessions begun after this command is issued. The default is disabled.

Syntax

```
enable tcp keepalives
```

Related Commands

[disable tcp keepalives](#)

[show tcp](#)

**enable tcp
nagle_algorithm**

This command allows use of the Nagle algorithm to limit small TCP packet transmissions and maintain high network throughput. This algorithm withholds additional packet transmissions to an output buffer until there is sufficient data to fill a maximum-sized segment. You may want to disable this feature if your TCP application must transmit small TCP packets. The default is enabled.

Syntax

```
enable tcp nagle_algorithm
```

Related Commands

[disable tcp nagle_algorithm](#)

[show tcp](#)

list tcp connections

This command displays information about all TCP (TELNET, RLOGIN, etc.) connections including those set by the user.

Syntax

```
list tcp connections
```

- **Local address**—IP address of the local host for this connection
- **Local Port**—TCP port number used by the local connection
- **Remote address**—IP address of the remote host for this connection
- **Remote Port**—TCP port number used by the remote connection
- **Status**—State of the connection. Values displayed are Closed, Listen, SynSent, SynReceived, Established, FinWait1, FinWait2, CloseWait, LastAck, Closing, TimeWait or DeleteTCB.

**set clearTCP
connect_message**

This command configures the string that is sent to ClearTCP clients, when the TCP connection is established. The message string must be enclosed in quotes. The limit is 64 ASCII characters.

Syntax

```
set clearTCP connect_message <message string>
```

Refer to the following conventions to follow when you compose the message.

If the string is surrounded by double quotes, you can insert an escape character '\ ' inside the quoted string. If the string is followed by the characters **b, f, n, r, t or v**, the router card places special characters in the string, as follows:

- **\b** = backspace
- **\f** = formfeed
- **\n** = newline
- **\r** = carriage return
- **\t** = tab
- **\v** = vertical tab

If the string is followed by an **x**, the next two characters are interpreted as a hexadecimal constant as follows:

- **x0A** = 0x0a

If the string is followed by *any other character*, that character is placed in the token.

Other rules state the following:

- A double quote (") places the double quote in the token.
- A forward slash '/' places one forward slash in the token.

**set tcp
keepalive_interval**

This command configures a period of inactivity (in seconds) on a TCP session after which a TCP keep-alive packet is sent on the session to learn whether it is still active. The inactive period begins after this command is issued. This command is used in conjunction with the [enable tcp keepalives](#) command. The range is 1 to 2147483 seconds. The enable/disable configuration is disabled by default.

Syntax

```
set tcp keepalive_interval <period>
```

Related Commands

[enable tcp keepalives](#)

[disable tcp keepalives](#)

[show tcp](#)

**set tcp
maximum_connections**

This command sets the total number of TCP connections the router card can support. TCP services include Telnet and ClearTCP. The range is 0 to 4096.

Syntax

```
set tcp maximum_connections <number>
```

show clearTCP

This command displays the ClearTCP message when a ClearTCP client session is connected to the remote TCP host.

Syntax

```
show clearTCP settings
```

show tcp This command displays system-wide TCP settings.

Syntax

```
show tcp settings
```



Most of these settings cannot be edited.

TCP Settings

- **Retransmission Algorithm**—Type of algorithm used
- **Minimum Timeout**—Minimum retransmission timeout interval
- **Maximum Timeout**—Maximum retransmission timeout interval
- **Maximum Connections**—Sum of TCP connections allowed
- **TCP Nagle Algorithm**—State of the Nagle algorithm which, when enabled, prohibits one octet-sized TCP packet transmissions to an output buffer until there is sufficient data to fill a maximum-sized segment. The default is enabled.
- **Keep-Alives**—Status of the keep-alive function
- **Keep-Alive Interval**—Period in seconds of receive inactivity before a keep-alive packet is sent

3

HOST AND SERVER COMMANDS

This chapter describes the following Host and Server Commands:

- [DHCP](#)
- [Login](#)
- [Ping](#)
- [RSHD](#)
- [SNMP](#)
- [TFTP](#)

DHCP

This section covers Dynamic Host Configuration Protocol (DHCP) commands of the CLI.

set dhcp_proxy

This command controls whether or not proxy leases are allowed and what happens when a proxy lease expires.

Syntax

```
set dhcp_proxy
    disc_if_lease_exp [no | yes]
    enabled [no | yes]
    retry <2 | 5>
```

Table 36 Set DHCP_Proxy Command Parameter Description

Parameter	Description
disc_if_lease_exp	When set to no, clients are not disconnected when their lease expires. When set to yes, clients are disconnected when their lease expires.
enabled	Allows (yes) or disallows (no) clients from receiving an address from the DHCP server.
retry	The number of retries before disconnecting.

Example

```
set dhcp_proxy disc_if_lease_exp yes enabled yes retry 2
```

Related Commands[show dhcp_proxy settings](#)[list dhcp_proxy leases](#)**show dhcp_proxy settings**

This command displays DHCP proxy status, lease disconnection state, and the number of client retries.

Syntax

```
show dhcp_proxy settings
```

Table 37 Show DHCP_Proxy Settings

Parameter	Description	Settings	Default
Status is	Displays whether DHCP proxy is enabled or disabled.	enabled disabled	enabled
Disconnect if Lease Expires	The status of the disconnect after lease expires feature.	enabled disabled	disabled
DHCP Proxy Client Retry	The current setting for the amount of times the DHCP proxy client will retry to connect.	2 to 5	2

Example

```
show dhcp_proxy settings
```

Related Commands[set dhcp_proxy](#)**list dhcp_proxy leases**

This command lists information about IP addresses that have been leased to clients.

Syntax

```
list dhcp_proxy leases
```

Example

```
list dhcp_proxy leases
```

Table 38 List DHCP_Proxy Leases

Parameter	Description
Index	The index number of the client.
Leased IP addr	The IP address leased to the corresponding index number.
LeaseTime Elapsed	The amount of time elapsed since the IP address lease has started.
ClientID	The client ID number.

show dhcp_proxy counters

This command displays DHCP proxy counter information.

Syntax

```
show dhcp_proxy counters
```

Table 39 Show DHCP_Proxy Counters

Parameters	Description
Proxy Discoveries sent	The sum of Proxy discoveries sent.
Proxy Offers received:	The number of proxy offers received.
Proxy IP Addresses acquired	The number of IP addresses released.
Proxy IP Addressed released	The number of IP addresses released.
Proxy Clients active	The number of active clients.
T1 Renewals sent	The sum of T1 renewals sent.
T2 Renewals sent	The sum of T2 renewals sent.

Example

```
show dhcp_proxy counters
```

Login

This section covers login commands of the CLI.

add login_host

This command adds up to 10 login hosts to the Login Host Table. You add login hosts so users of type *login* connecting to an IP host can reference the host by name. The system looks up the address, using the DNS server you define with the add DNS server command. Or, you can specify the IP address here. Display the currently defined login hosts with the list login_hosts command.

Syntax

```
add login_host <hostname>
    address <IP address>
    preference <number>
    rlogin_port <TCP port number>
    clearTCP_port <TCP port number>
```

Table 40 Add Login_Host Parameter Descriptions

Parameter	Description	Settings	Default
host name	The name or IP address that specifies an IP host.	Up to 32 ASCII characters	—
address	<i>Optional.</i> The address of login host. If you do not specify an address here, the system will consult the DNS server to find the address.	xxx.xxx.xxx.xxx	—
preference	Priority of the login host. Each host can be assigned a unique preference number for selection by the server. The first preference is 1, and 10 is the last.	1 to 10	—

Table 40 Add Login_Host Parameter Descriptions

Parameter	Description	Settings	Default
rlogin_port	<i>Optional.</i> Specifies the port number that will be used when a user executes the rlogin CLI command, specifying this host.	1 to 65535	513
telnet_port	<i>Optional.</i> The port number used when a user executes the telnet CLI command, specifying this host.	1 to 65535	23
clearTCP_port	<i>Optional.</i> The port number used when a user's application requests a ClearTCP session with this host.	1 to 65535	6000

Example

```
add login_host chicago address 10.10.3.3 preference 2 rlogin_port
514 telnet_port 24 clearTCP_port 6001
```

Related Commands

[delete login_host preference](#)

[list login_hosts](#) set login_host preference

delete login_host preference

This command removes the login host with the specified preference, 1 (first) to 10 (last).

Syntax

```
delete login_host preference <preference number>
```

Example

```
delete login_host preference 9
```

Related Commands

[add login_host](#)

[list login_hosts](#) set login_host preference

add login_table This command creates a login table. To set a login table to a switched interface, refer to set switched interface login_table. To set a login table to a modem group, refer to set modem_group login_table.

Syntax

```
add login_table <name>
    address <IP address>
    port <port number>
    preference <number>
```

Table 41 Add Login_table Parameter Description

Parameter	Description	Settings
address	IP address of the login host of the login host table.	Up to 32 ASCII characters.
port	Port number of the login host of the login host table.	1 to 65535
preference	Assigns a preference of value. When the router card uses the login table, it tries each IP address port value pairs starting with preference 1 to 10 until it gets a connection or the login host table entries are finished.	1 (first) to 10 (last)

Example

```
add login_table chicago address 10.10.3.3 port 3000 preference 4
```

Related Commands

```
set switched interface login_table
set modem_group login_table
```

list login_table This command shows the name, IP address, and port number of available login tables.

Syntax

```
list login_table
```

Example

```
list login_table
```

Related Commands

[add login_table](#)
[delete login_table](#)

delete login_table This command removes the login table with the specified preference number. Refer to [add login_table](#) command to create login_tables. Use [list login_table](#) to see the available login hosts and their associated port and preference numbers.

Syntax

```
delete login_table <name> preference <preference>
```

Example

```
delete login_table chicago preference 2
```

Related Commands

[add login_table](#)

[list login_table](#)

disable prompting single_level This command disables “first level” CLI prompting of Login/Network users by the router card. When enabled, this function bypasses the Login/Network prompt for those users, delivering them directly to the prompt line, but still allows all first level accessed services such as telnet, rlogin, traceroute, etc.

This command is disabled by default.

Syntax

```
disable prompting single_level
```

Example

```
disable prompting single_level
```

Related Commands

[enable prompting single_level](#)

[show prompting](#)

disable rlogin escape This command disables the use of escape keys for rlogin users.

This is enabled by default.

Syntax

```
disable rlogin escape
```

Example

```
disable rlogin escape
```

Related Commands

[enable rlogin escape](#)

**enable prompting
single_level**

Enables “first level” CLI prompting of Login/Network users by the router card. This function bypasses the standard *Login/Network* prompt for those users, depositing them directly at the *HiPer>* prompt line where the *Network* keyword can be issued. The command still permits all first level accessed services such as TELNET, RLogin, traceroute, etc., and lets properly configured Login/Network users invoke a PPP session *after* completing any TELNET/RLogin/ClearTCP sessions, if desired. After the PPP session ends, though, the connection is terminated.

This feature is disabled by default.

Syntax

```
enable prompting single_level
```

Example

```
enable prompting single_level
```

Related Commands

[disable prompting single_level](#)

[show prompting](#)

enable rlogin escape

This command enables the use of escape keys for rlogin users.

This feature is enabled by default.

Syntax

```
enable rlogin escape
```

Example

```
enable rlogin escape
```

Related Commands

[disable rlogin escape](#)

list login_hosts

This command displays currently defined entries in the Login Host Table previously defined using [add login_host](#).

Syntax

```
list login_hosts
```

Table 42 List Login Hosts Description

Parameter	Description
Preference	The priority preference number assigned to the host.
Name	The name assigned to the login host.
Rlogin, telnet, and ClearTCP Ports	The rlogin, telnet, and ClearTCP port numbers assigned to that login host.

Example

```
list login_hosts
```

Related Commands

[add_login_host](#)

[delete_login_host_preference](#) set login_host preference

list login_sessions

This command lists all login sessions when DNS is enabled. It displays the username and the host to which that user is logged in. If a user is logged in on more than one session, it lists each session separately.

This command is useful when DNS host rotation is enabled and multiple instances of the same user are logged in to different hosts using DNS host rotation.

Syntax

```
list login_sessions
```

Example

```
list login_sessions
```

resolve name

This command returns an IP address for the specified host name by sending it to DNS for resolution. If the Domain Name has been specified using the [set dns](#) command, it is also resolved. Otherwise you must specify it as part of the name.

This command requires either a DNS local host ([add dns host](#)) or a DNS server entry ([add dns server](#)) to resolve the name. This command is identical to the [host <IP host name>](#) command.

Syntax

```
resolve name <host name>
```

Example

```
resolve name chicago
```

Related Commands

[set dns](#)

[add dns host](#)

[add dns server](#)

[host <IP host name>](#)

rlogin This command creates an rlogin client connection to the specified host.

Syntax

```
rlogin <host name or IP address>
      login_name <login name>
      TCP_port <port number>
```

Table 43 Rlogin Command Description

Parameter	Description	Settings	Default
<host name or IP address>	Either the IP address or the host name of the remote system.	IP: xxx.xxx.xxx.xxx Host name: up to 64 ASCII characters.	—
login name	User name needed to login to the remote system.	Up to 64 ASCII characters.	—
TCP port	TCP port number to create the connection to. The default is 513 . The maximum is 65535 .	1 to 65535	513

Example

```
rlogin 10.10.3.3 login_name user1 TCP_port 9000
```

set login_host preference This command sets rlogin, telnet, or ClearTCP ports for a specified login host. The specified port number is used by the login host to accept connections using that method.

Syntax

```
set login_host preference <preference number>
      rlogin_port <port number>
      telnet_port <port number>
      clearTCP_port <port number>
```

Table 44 Set Login_host Preference Description

Parameter	Description	Settings	Default
<preference number>	Defines preferred rank in which a login host will be used. Use list login_hosts to see the preference number associated with a login host.	1 (first) to 10 (last)	
rlogin_port	TCP port number you wish to configure for Rlogin access to the login host. If you do not specify it here, and the user does not specify the TCP port from the CLI rlogin command, then the default is 513.	1 to 65535	513
telnet_port	TCP port number you wish to configure for TELNET access to the login host. If you do not specify it here, and the user does not specify the TCP port from the CLI telnet command, then the default is 23.	1 to 65535	23
clearTCP_port	TCP port number you wish to configure for ClearTCP access to the login host. There is no default TCP port number.	1 to 65535	6000

Example

```
set login_host preference 1 rlogin_port 9000 telnet_port 9001
clearTCP_port 9002
```

Related Commands

[add_login_host](#)
[delete_login_host_preference](#)
[list_login_hosts](#)

set login_table <name> This command changes the existing value of a login table parameter.

Syntax

```
set login_table <name>
  preference <number>
  addr <IP address>
  port <port_no>
```

Table 45 Set Login_table Command Parameter Descriptions

Parameter	Description	Settings
IP address	IP address of the login host with the login host table.	xxx.xxx.xxx.xxx
port	Port number assigned to the login host.	1 to 65535
preference	When the router card uses the login table, it tries each IP address port value pairs starting with preference 1 to preference 10 until it gets a connection or the login host table entries are finished.	1 (first) to 10 (last)

Example

```
set login_table main2 preference 2 addr 10.10.3.3 port 9000
```

show prompting This command displays the type of CLI prompting specified for Login/Network users on the router card. When configured by the [enable prompting_single_level](#) command, the *Login/Network* prompt is bypassed for those users—they are deposited directly at the *HiPer>* prompt line.

Syntax

```
show prompting
```

Example

```
show prompting
```

Related Commands

[disable prompting_single_level](#)

[enable prompting_single_level](#)

Ping**add ping
service_loss_system**

This command creates a configurable ping that monitors IP connectivity across the network to a specified server. If service is lost to the server, the router card notifies the NMC (which can be configured) to use auto-response to busy out all chassis modems so no more calls are answered and any hunt groups will answer to other systems.

Based on the ICMP ping protocol, this command checks the IP address for each time period specified. If no response is received before the timeout expires, the router card busies out all modems. Pings continue after modems busy out and when connectivity to all modems is restored, modem service is restored

Syntax

```

add ping service_loss_system <IP address>
    enabled [yes | no]
    frequency <1 to 200>
    misses_allowed <1 to 1000>
    timeout <1 to 6000>

```

Table 46 Add Ping Service_Loss_System Command Parameter Descriptions

Parameter	Description	Settings	Default
<ip name or address>	IP name or address of the system to be pinged.	xxx.xxx.xxx.xxx	—
enabled	Ping service enabled/disabled to particular server.	yes no	—
frequency	Interval in seconds between ping requests.	1 to 200	30
misses_allowed	Number of ping failures allowed before busying out modems.	1 to 10	1
timeout	Interval in seconds to wait before busying out modems.	1 to 60	10

Example

```

add ping service_loss_system 10.10.3.3 enabled yes frequency 5
misses_allowed 10 timeout 100

```

Related Commands

[delete ping service_loss_system](#)

[disable ping service_loss_system](#)

[enable ping service_loss_system](#)

[list ping service_loss_systems](#)

[set ping service_loss_system](#)

[show ping server <host name or IP address> settings](#)

[show ping server <host name or IP address> settings](#)

delete ping row This command deletes the specified ping row from the Remote Ping Table.

Syntax

```

delete ping row <0 to 65535>

```

Example

```

delete ping row 8

```

**delete ping
service_loss_system**

This command deletes server connectivity pinging to specified IP name or address.

Syntax

```
delete ping service_loss_system <host name or IP address>
```

Example

```
delete ping service_loss_system 10.10.3.3
```

**disable ping
service_loss_system**

This command disables the router card ability to repeatedly ping the specified system to check for connectivity.

Syntax

```
disable ping service_loss_system <host name or IP address>
```

Example

```
disable ping service_loss_system 10.10.3.3
```

Related Commands

[enable ping service_loss_system](#)

[list ping service_loss_systems](#)

**enable ping
service_loss_system**

This command enables the router card to repeatedly ping the specified system to check for connectivity. Use the show service_loss_system settings command to view edits.

Syntax

```
enable ping service_loss_system <host name or IP address>
```

Example

```
enable ping service_loss_system 10.10.3.3
```

Related Commands

[disable ping service_loss_system](#)

[list ping service_loss_systems](#)

**list ping
service_loss_systems**

This command displays information from systems pinged as specified by the [add ping service_loss_system](#) command.

Syntax

```
list ping service_loss_systems
```

Table 47 List Ping Service_loss_systems Description

Parameter	Description
Name	IP address of the system to ping.
Freq	Number of seconds between ping requests.

Table 47 List Ping Service_loss_systems Description

Parameter	Description
Time	Number of seconds a ping request can be open before it fails (is labeled a miss).
Miss	Number of allowable misses before the system is deemed unreachable.
Status	Status of the server pinged, either enabled or disabled.

Example

```
list ping service_loss_systems
```

Related Commands

[disable ping service_loss_system](#)

[enable ping service_loss_system](#)

list ping systems

This command displays the results of ping, including data from the Remote Ping Table.

Syntax

```
list ping systems
```

Table 48 List Ping Display Information

Parameter	Description
Row	The row number within the Remote Ping Table.
Destination	Host name or IP address of the target node being tested.
Status	Present state of this row. Possible states include: <ul style="list-style-type: none"> ■ Complete—requested number of pings resolved. ■ Active—ping requests in progress. ■ Bad address—resolved IP address is illegal. ■ Waiting DNS—awaiting DNS resolution. ■ Not Active—specified ping row not active. ■ DNS Failed—destination address could not be resolved. ■ Alloc Failed—system failed to allocate resources.
Count	The number of pings to be transmitted.
Interval	The number of seconds between ping requests.
Size	In bytes, the size of data to be transmitted.
TTL	The ping message time-to-live period

Example

```
list ping systems
```

Related Commands

[ping](#)

ping This command sends a ping (ICMP echo request) to a remote IP host. This tool tests connectivity and can also be initiated from an SNMP station. The CLI can perform a ping with either verbose or background selected, but not both.

Verbose causes the CLI to display information for each PING transmitted. *Background* causes the CLI to start the PING request and returns you to the prompt until results are ready.

The ping command is paused during execution using the following keys:

- S or ENTER continues printing
- q cancels rest of output
- Ctrl C quits output

Syntax

```
ping <host name or IP address>
    background [yes | no]
    count <maximum packets>
    data <string>
    interval <seconds>
    self_destroy_delay <minutes>
    size <data size>
    timeout <period>
    verbose [yes | no]
```

Table 49 Ping Parameter Description

Parameter	Description	Settings	Default
host name or IP address	The IP address or host name of the remote system.	xxx.xxx.xxx.xxx	—
background	When selected, pings are run in a background process on your screen. This setting can run in either background or verbose mode, but not both.	yes no	no
count	The number of pings requests to send.	1 to 1000	1
data	String value specifying data to be sent. Note: If data length is bigger than ping size, only the first ping size octets are used. If data length is zero, the server uses random data. If data length is smaller than ping size, the data pattern will be repeated as many times as necessary to fill up the transmission buffer.	Up to 256 ASCII characters	—
interval	The period in seconds between successive ping requests. Note that the actual interval might be different for any given transmission, because the server will not send a new request before a previous request is completed (replied to or timed-out).	1 to 65535 seconds.	1 second

Table 49 Ping Parameter Description

Parameter	Description	Settings	Default
self_destroy_delay	When <i>background</i> is selected, the period indicating the number of minutes a row in the Remote Ping Table is allowed to be inactive before it is erased by the server. A row is considered inactive any time the ping state is one of the following: <ul style="list-style-type: none"> ■ Not Active—row is not active ■ DNS Failed—destination address could not be resolved ■ Bad address—resolved IP address is illegal ■ Completed—requested number of iterations is completed ■ Alloc Failed—failed to allocate resources 	0 to 65535 minutes.	10 minutes
size	The size of pinged packet. Note that the actual datagram is larger than this value by 42 octets because it includes: <ul style="list-style-type: none"> ■ MAC header (14 octets on Ethernet) ■ IP header (20 octets) ■ ICMP header (8 octets) 	1 to 1400 bytes	64 bytes
timeout	The period in seconds before determining a transmission has not been replied to. The range is 1 to 60. The default is 20 seconds.	1 to 60 seconds	20 seconds

Example

```
ping 10.10.3.3 background yes count 100 timeout 10
```

Related Commands

[list ping systems](#)

set ping maximum_rows

This command sets the maximum number of rows permissible in the Remote Ping Table. Note that setting this parameter to a number smaller than the current number of rows will not cause any row deletions immediately, but will effect it in the future. Use the [show ping settings](#) command to view configuration.

Syntax

```
set ping maximum_rows <1 to 20>
```

Example

```
set ping maximum_rows 100
```

Related Commands

[show ping settings](#)

**set ping
service_loss_system**

This command sets parameters configured by the [add ping service_loss_system](#) command. Use the [list ping service_loss_systems](#) command to display configuration. This command creates a configurable ping that monitors IP connectivity across the network to a specified server. If service is lost to the server, the router card notifies the NMC (which can be configured) to use auto-response to bust-out all chassis modems so no more calls are answered and any hunt groups will answer to other systems. Based on the ICMP ping protocol, this command checks the IP address for each time period specified. If no response is received before the timeout expires, the router card busies-out all modems. Pings continue after modems busy-out and when connectivity to all modems is restored, modem service is restored

Syntax

```
set ping service_loss_system <host name or IP address>
    frequency <1-200>
    misses_allowed <1-1000>
    timeout <1-6000>
```

Table 50 Set Ping Service_Loss_System Command Parameter Descriptions

Parameter	Description	Settings	Default
<ip name or address>	IP name or IP address of the system you want pinged.	xxx.xxx.xxx.xxx or Up to 64 ASCII characters.	—
frequency	The number of seconds between ping requests.	1 to 200	30
misses_allowed	The number of ping failures allowed before busying out modems.	1 to 10	1
timeout	Interval in seconds to wait before busying out modems.	10	1 to 60

Example

```
set ping service_loss_system 10.10.3.3 frequency 10
misses_allowed 50 timeout 100
```

show ping settings

This command displays general ping settings.

Syntax

```
show ping settings
```

Example

```
show ping settings
```

Related Commands

[ping](#)
[set ping maximum_rows](#).

show ping row This command displays settings for the specified row in the Remote Ping Table. These settings reflect the configuration specified with the [ping](#) command.

Syntax

```
show ping row <1 to 1000> settings
```

Example

```
show ping row 1 settings
```

Related Commands

[ping](#)

show ping server settings This command displays ping server settings specified with [add ping service loss system](#). A value of -1 indicates failure of ping system.

Syntax

```
show ping server settings
```

Table 51 Show Ping Server Settings Description

Parameter	Description	Settings	Default
Status	Whether the system is being pinged regularly or not.	enabled disabled	enabled
Frequency	The interval in seconds between each ping request.	1 to 65535	30
Misses Allowed	The number of ping messages that can be missed before modems are busied out.	1 to 65535	1
Time Out	How long a ping request can be outstanding before it is considered to have failed.	1 to 65535	2
Reachable	Whether or not the ping server is connected.	yes no	—
Time Contacted	The number of seconds since the server was reached.	1 to 65535	—
Address	The IP address of the system	xxx.xxx.xxx.xxx	—

Example

```
show ping server settings
```

Related Commands

[add ping service loss system](#)

show ping server <host name or IP_address> settings

This command displays the same server settings as the [show ping settings](#) command but for a specified host or IP address.

Syntax

```
show ping server <host name or IP address> settings
```

Example

```
show ping server 10.10.3.3. settings
```

Related Commands

[show ping settings](#)

RSHD

This section addresses commands to add, delete, and list remote shell clients.

add rshd clients

This command adds a new remote shell client IP address and user name. Both the IP address and user name must be specified.



For rsh security reasons, only users from the specified IP address with the specified username will be allowed to make rsh/rcp connections. If you specify an ip address of 0.0.0.0 and an empty string for the user name ("") everyone is granted access.

Syntax

```
add rshd clients ip_address <host name or IP address>
user_name <up to 64 ASCII characters>
```

Example

```
delete rshd clients ip_address 10.10.3.3 user_name smith
```

Related Commands

[delete rshd clients](#)

delete rshd clients

This command deletes the specified remote shell client IP address and user name.

Syntax

```
delete rshd clients ip_address <host name or IP address>
user_name <any existing user name>
```

Example

```
delete rshd clients ip_address 10.10.3.3 user_name smith
```

Related Commands

[add rshd clients](#)

list rshd clients This command list all configured remote shell clients' user names and IP addresses.

Syntax

```
list rshd clients
```

Example

```
list rshd clients
```

Related Commands

[add rshd clients](#)

[delete rshd clients](#)

SNMP

This section addresses commands that handle Simple Network Management Protocol (SNMP) functionality.

add snmp community This command adds to a table of SNMP-authorized users. If you do not want to restrict SNMP access to a particular IP address, specify the address as "0.0.0.0" (public). The community name and IP address of SNMP requests from managers on the network must match the list, which you can see using [list snmp communities](#).

Multiple management stations can manage the router card using the same SNMP community name by use of the SNMP Community address Pool table, which associates a community name with IP addresses.

Syntax

```
add snmp community <community name>
    address <IP_address>
    access [ro | rw | adm]
    community_pool <name>
    validate_address [use_address | use_pool]
```

Table 52 Add SNMP community Command Parameter Descriptions

Parameter	Description	Settings	Default
community name	The group name that authorizes SNMP requests.	Up to 64 ASCII characters.	—
address	IP address of the remote SNMP manager.	xxx.xxx.xxx.xxx	—
access	Determines what type of access to SNMP MIBs the specified user has.	Read Only (RO)— user-level objects Read Write (RW)— user-level objects Administrator (ADM)— Administrator allows <i>read access to all objects</i> and <i>write access to all writable objects</i> .	RO is the default on public (0.0.0.0) networks and RW is the default on private networks.
community pool	The name of the SNMP community pool to use.	Any valid pool name.	—
validate_address	When set to <i>use_address</i> the address of the SNMP community is used to validate the management station's IP address. When set to <i>use_pool</i> , the management station's IP address is validated against the list of IP address associated with the <i>community_pool</i> .	use_address use_pool	use_address

Example

```
add snmp community office address 10.10.3.3 access ro
community_pool
```

add snmp community_pool

This command adds an entry to the SNMP community address pool table, used in conjunction with the [add snmp community](#) command to allow multiple management stations control of the router card using a pool of IP addresses.

Syntax

```
add snmp community_pool <pool name>
address <host name or IP address>
```

Table 53 Add SNMP Community_pool Parameter Descriptions

Parameter	Description
pool name	Pool name defining a group of SNMP management stations. The limit is 10 .
address	IP name or address of an SNMP management station in the pool. The limit is 10 .

Example

```
add snmp community_pool pool1 address 10.10.3.3
```

**add snmp
trap_community**

This command adds to the list of community name/IP address pairs that are allowed to receive SNMP traps, as well as allows multiple management stations to use the same SNMP trap community name. Entries are added to the SNMP Trap Community Address Pool table. You can display authorized users with the [list snmp communities](#) command.

Syntax

```
add snmp trap_community <name>
    address <IP address>
    trap_community_pool <name>
    trap_validate_address [use_address | use_pool]
```

Table 54 Add SNMP Trap_Community Command Parameter Descriptions

Parameter	Description	Settings	Default
name	The group name defining who can receive SNMP traps.	Up to 64 ASCII characters.	—
IP address	IP address of the SNMP manager, in the form <i>nnn.nnn.nnn.nnn</i> .	xxx.xxx.xxx.xxx	—
trap_community_pool	The name of the trap community pool.	Up to 64 ASCII characters.	—
trap_validate_address	When set to <i>use_address</i> (default), the <i>address</i> of the SNMP trap community is used to validate the management station's IP address. When set to <i>use_pool</i> , the management station's IP address is validated against the list of IP addresses associated with the <i>trap_community_pool</i> . Employing <i>use_pool</i> selects IP addresses from the pool as destination addresses and does not use the specified <i>address</i> parameter although a token address must be entered for purposes of backward compatibility.	use_address use_pool	use_address

Example

```
add snmp trap_community comm1 address 10.10.3.3
trap_validate_address use_address
```

Related Commands

[list snmp communities](#)

add snmp trap_community_pool

This command adds up to four or eight entries at a time (depending on the number of characters each IP address occupies) to the SNMP Trap Community Address Pool table. If IP addresses are in the single-digit form (e.g. 1.1.1.1), eight entries can be added with the single CLI command; if addresses are in triple-digit form (e.g. 146.115.112.111), four IP addresses can be added with the single CLI command. The maximum size of the pool is 10 IP addresses

Syntax

```
add snmp trap_community_pool <name>
addresses <IP address list>
```

Table 55 Add SNMP Trap Community Pool Command Parameter Descriptions

Parameter	Description
<name>	Pool name defining who can receive SNMP traps.
addresses	IP addresses of all SNMP managers associated with the pool, in xxx.xxx.xxx.xxx format, separated by a comma.

Example

```
add snmp trap_community_pool comm2 addresses 10.10.3.3,10.10.3.20
```

Related Commands

[delete snmp community_pool](#)

[list snmp community_pools](#)

delete snmp community

This command removes an SNMP community that was previously added with the [add snmp community](#) command. You can use [list snmp communities](#) to see the current entries.

Syntax

```
delete snmp community <name>
```

Example

```
delete snmp community comm2
```

**delete snmp
community_pool**

This command removes an entry from the SNMP community address pool table. See the `add snmp community` command for more information.

Syntax

```
delete snmp community_pool <pool name>
address <host name or IP address>
```

Table 56 Delete SNMP Community_Pool Command Parameter Descriptions

Parameter	Description
<pool_name>	Pool name defining a group of SNMP management stations.
address	IP address or name of an SNMP management station in the pool.

Example

```
delete snmp community_pool comm2
```

**delete snmp
trap_community**

This command removes an SNMP trap community name from the list of names and IP addresses that are allowed to receive SNMP trap commands. You can use [list snmp communities](#) to see the current entries.

Syntax

```
delete snmp trap_community <name>
```

Example

```
delete snmp trap_community comm2
```

Related Commands

[list snmp communities](#)

**delete snmp
trap_community_pool**

This command removes entries from the SNMP Trap Community Address Pool table. See [add snmp trap community pool](#) and [list snmp community pools](#) commands for more information.

Syntax

```
delete snmp trap_community_pool <name>
addresses <IP address list>
```

Table 57 Delete SNMP Trap Community Pool Parameter Descriptions

Parameter	Description
name	The pool name defining who can receive SNMP traps.
addresses	IP addresses of all SNMP managers associated with the pool in xxx.xxx.xxx.xxx format.

Example

```
delete snmp trap_community_pool comm2 10.10.3.3
```

disable link_traps interface

This command prevents SNMP from sending linkup and linkdown traps for the specified interface or modem group. We recommend you disable this feature on all *modem* interfaces to eliminate messages forwarded from the network management card. Although the default is disabled on modem interfaces, Hubs with *Quad Modems* installed must have the router card setting disabled manually to effect the change. The command is enabled for Ethernet and WAN connections.

Syntax

```
disable link_traps interface  
    interface_name <eth:1, eth:2 or slot:x/mod:y>  
    modem_group <name>
```

Related Commands

[enable_modem_group](#)
[show_rs232_interface](#)

disable security_option snmp user_access

This command disables SNMP access to the system. This prevents remote users from using SNMP and damaging the configuration. Use [enable_security_option_snmp_user_access](#) to enable full SNMP access.

Syntax

```
disable security_option snmp user_access
```

Example

```
disable security_option snmp user_access
```

Related Commands

[enable_security_option_snmp_user_access](#)

disable snmp authentication traps

This command instructs SNMP to stop recording trap information for user (either local or remote) authentication.

Related Commands

[enable_snmp_authentication_traps](#)
[show_snmp_trap_community_pool](#)

**enable link_traps
interface**

This command informs SNMP to send linkup and linkdown traps for the specified interface or modem group. We recommend you disable this feature on all *modem* interfaces to eliminate a barrage of perfunctory awareness messages forwarded from the NMC to the router card alarm server whenever modem states change or the router card reboots.



Although the default is disabled on modem interfaces, Hubs with Quad Modems installed must have the router card setting disabled manually to effect the change. The command is enabled for Ethernet and WAN connections.

Syntax

```
enable link_traps interface
    interface_name <eth:1, eth:2 or slot:x/mod:y>
    modem_group <name>
```

Example

```
enable link_traps interface interface_name eth:2
```

Related Commands

[disable link_traps interface](#)

[show interface <interface name> settings](#)

**enable security_option
snmp user_access**

This command allows SNMP access to the User Table. This lets remote users use SNMP to access the CLI and reconfigure the router card. Use [show security options](#) to see the current security values.

Syntax

```
enable security_option snmp user_access
```

Example

```
enable security_option snmp user_access
```

Related Commands

[show security options](#)

**enable snmp
authentication traps**

This command informs SNMP to send traps for both local and remote authentication. The default is enabled.

Syntax

```
enable snmp authentication traps
```

Example

```
enable snmp authentication traps
```

Related Commands

[disable snmp authentication traps](#)

[show snmp trap_community_pool](#)

list snmp communities This command displays the SNMP communities defined using the [add snmp community](#) command.

Syntax

```
list snmp communities
```

Table 58 List SNMP Communities Description

Parameter	Description
Community Name	The community designation for the IP address.
IP Address	The IP address of a member of the community.
Access	The allowed access granted for this community. Values: <ul style="list-style-type: none"> ■ Read/Only—read only access to user-level objects. ■ Read/Write—read and write access to user-level objects, and write access to writable user-level objects allowed. ■ Administrator—read access to all objects and write access to all writable objects allowed.
Community Pool	The name for a pool of IP addresses comprising this SNMP community.
Validate Address	The method selected to determine access to this community. The <code>use_address</code> command uses the specified IP address to validate access, <code>use_pool</code> uses the list of IP addresses specified in the <code>community_pool</code> value to validate access.

Example

```
list snmp communities
```

list snmp community_pools This command displays the name and number of addresses for all entries in the SNMP Community address Pool table. Refer to [add snmp community_pool](#) command for more information.

Syntax

```
list snmp community_pools
```

Example

```
list snmp community_pools
```

Related Commands

[add snmp community_pool](#)

**list snmp
trap_communities**

This command displays SNMP trap communities defined using the [add snmp trap_community](#) command.

Syntax

```
list snmp trap_communities
```

Table 59 List SNMP Trap_communities Description

Parameter	Description
Community Name IP Address	The trap community designation for the associated system.
Community Pool	The name of the trap community pool. If the trap community pool does not exist and the validate_address parameter is configured to use the trap community pool, the name of the trap community pool displayed is preceded by an asterisk.
Validate Address	The method selected to determine access to this trap community. The use_address command uses a specified IP address to validate access, use_pool uses a list of IP addresses to validate access.

Example

```
list snmp trap_communities
```

Related Commands

[add snmp trap_community](#)

**list snmp
trap_community_pools**

This command displays all SNMP trap community pools in the SNMP Trap Community Address Pool defined using [add snmp trap_community_pool](#). It lists the following information:

- **Name**—designation of the trap community pool.
- **Number of Addresses**—Sum of IP addresses associated with the specified trap community pool.

Syntax

```
list snmp trap_community_pools
```

Example

```
list snmp trap_community_pools
```

set snmp community This command modifies parameters for an SNMP community (authorized user or host to which notifications are sent) configured with the [add snmp community](#) command. The community name and IP address of SNMP requests from managers on the network must match the list, which you can view using [list snmp communities](#).

Syntax

```
set snmp community <name>
    access [ro | rw | adm]
    address <IP_address>
    community_pool <name>
    validate_address [use_address | use_pool]
```

Table 60 Set SNMP Community Command Parameter Descriptions

Parameter	Description	Setting	Default
name	The group designation for a pool of management stations which authorize SNMP requests.	Any valid SNMP community name.	—
access	Determines what type of access to SNMP MIBs the added user will have. Options are Read Only (RO), Read Write (RW) and Administrator (ADM).	RO—read-only RW—read-write ADM—admin Administrator allows read access to all objects and write access to all writable objects.	RO is the default on public (0.0.0.0) networks and RW the default on private networks.
address	IP address of this SNMP management station.	xxx.xxx.xxx.xxx	—
community_pool	Designation for the pool of IP addresses comprising this SNMP community.	Up to 64 ASCII characters.	—
validate_address	Method to determine access to this management station. The <i>use_address</i> value uses the specified IP address to validate access. The <i>use_pool</i> value uses the list of IP addresses specified in the <i>community_pool</i> value to validate access.	use_address use_pool	—

Example

```
set snmp community comm1 access rw address 10.10.3.3
community_pool pool1 validate_address use_pool
```

Related Commands

[add snmp community](#)

[list snmp communities](#)

**set snmp
trap_community**

This command modifies parameters for an SNMP trap community (authorized user or host to which trap notifications are sent). The community name and IP address of SNMP requests from managers on the network must match the list, which you can view using [list snmp trap communities](#).

Syntax

```
set snmp trap_community <community name>
address <IP_address>
trap_community_pool <name>
trap_validate_address [use_address | use_pool]
```

Table 61 Set SNMP Trap_Community Command Parameter Descriptions

Parameter	Description	Settings
<community name>	Trap group designation for a pool of management stations which authorize SNMP requests.	
address	IP address of this SNMP management station	xxx.xxx.xxx.xxx
community_pool	Designation for the trap pool of IP addresses comprising this SNMP community. The limit is 64 ASCII characters.	Up to 64 ASCII characters.
trap_validate_address	Method to determine access to this management station. The <i>use_address</i> value uses the specified IP address to validate access. The <i>use_pool</i> value uses the list of IP addresses specified in the <i>trap_community_pool</i> value to validate access.	use_address use_pool

Example

```
set snmp trap_community address 10.10.3.3
```

show snmp settings

This command displays whether the SNMP Authentication Traps setting is enabled or disabled to indicate authentication-failures. The default is enabled.

Syntax

```
show snmp settings
```

Example

```
show snmp settings
```

Related Commands

[disable snmp authentication traps](#)

[enable snmp authentication traps](#)

show snmp community_pool This command displays the IP address of the specified SNMP community address pool.

Syntax

```
show snmp community_pool <pool_name>
```

Example

```
show snmp community_pool pool2
```

Related Commands

[add snmp community_pool](#)

show snmp trap_community_pool This command displays the specified SNMP trap community and IP addresses of associated trap communities defined using the [add snmp trap_community](#) command.

Syntax

```
show snmp trap_community_pool <name>
```

Example

```
show snmp trap_community_pool trapool2
```

TFTP

add tftp client This command adds the tftp client to the Authorization Table for TFTP access.

Syntax

```
add tftp client <IP address name>
```

Example

```
add tftp client 10.10.3.3
```

add tftp request This command adds entries to the TFTP Client Request Table. Entries are the names of files either requested *from* or sent *to* the TFTP server. The command is useful for administrators at SNMP management stations seeking to access the TFTP client router card.

Syntax

```
add tftp request <input_file_name>
    action [get | put]
    server <IP_name_or_IP_address>
    mode [ascii | octet]
    rexmt_timeout <1-60>
    max_timeout <1-300>
```

Table 62 Add TFTP Request Command Parameters Descriptions

Parameter	Description	Settings	Default
<input_file_name>	Designation of file to be requested from or sent to the TFTP server.	Up to 32 ASCII characters.	—
action	Type of request sent to the TFTP server.	put get	—
server	Name or IP address of the TFTP server.	xxx.xxx.xxx.xxx or host name	—
mode	The text format the file is transmitted as.	ascii octet	ascii
rexmt_timeout	Retransmission timeout - interval in seconds the router card waits for a reply from the TFTP server before retransmitting a TFTP request.	1 to 60	5
max_timeout	Interval in seconds the router card waits for a response from the TFTP server before the TFTP request is cancelled.	1 to 300	25

Example

```
add tftp request req action put server 10.10.3.3 mode ascii
rexmt_timeout 5 max_timeout 30
```

Related Commands

[disable tftp request](#)

[enable tftp request](#)

[list traceroute](#)

delete tftp client This command removes the specified IP host name or IP address from the list of addresses authorized to TFTP. Use [list tftp clients](#) to see the currently allowed addresses.

Syntax

```
delete tftp client <IP_name or address>
```

Example

```
delete tftp client 10.10.3.3
```

Related Commands

[list tftp clients](#)

delete tftp request This command removes specified TFTP entries in the TFTP Client Request Table created with the [add tftp request](#) command.

Syntax

```
delete tftp request <input_file_name>
```

Example

```
delete tftp request req2
```

Related Commands

[add tftp request](#)

disable tftp request This command deactivates a request for service (get or put) from the TFTP server created with the [add tftp request](#) command.

Syntax

```
disable tftp request <input_file_name>
```

Example

```
disable tftp request req2
```

Related Commands

[add tftp request](#)

[enable tftp request](#)

[list traceroute](#)

enable tftp request This command activates a request for service (get or put) from the TFTP server created with the [add tftp request](#) command. Use the list tftp request command to display TFTP request status.

Syntax

```
enable tftp request <input_file_name>
```

Example

```
enable tftp request req2
```

Related Commands

[add tftp request](#)

[disable tftp request](#)

[list traceroute](#)

list tftp clients This command displays IP addresses of all users allowed to use the Trivial File Transfer Protocol (TFTP) to connect to the system. Use the [add network service](#) command to add TFTP support to the system, the [add tftp client](#) to authorize users to connect and the [add tftp request](#) command to initiate TFTP service.

Syntax

```
list tftp clients
```

Example

```
list tftp clients
```

Related Commands

[add tftp request](#)

[add tftp client](#)

[add network service](#)

set tftp request This command configures requests to the TFTP server created with the [add tftp request](#) command. Entries placed in the TFTP Client Request Table are the names of files that are either requested from or sent to the TFTP server.

Syntax

```
set tftp request <input_file_name>
  action [get | put]
  max_timeout <1 to 300>
  mode [ascii | octet]
  rexmt_timeout <1 to 60>
  server <IP name or IP address>
```

Table 63 Set TFTP Request Command Parameter Descriptions

Parameter	Description	Settings	Default
<input_file_name>	Designation of file to be requested from or sent to the TFTP server.	Up to 64 ASCII characters.	—
action	Type of request sent to the TFTP server.	put get	—
max_timeout	Interval in seconds the router card waits for a response from the TFTP server before the TFTP request is cancelled.	1 to 300	25
mode	The text format the file will be transmitted as.	ascii octet	ascii
rexmt_timeout	Retransmission timeout - interval in seconds the router card waits before retransmitting a TFTP request.	1 to 60	5
server	Name or IP address of the TFTP server.	xxx.xxx.xxx.xxx	—

Example

```
set tftp request req2 action put max_timeout 50 mode ascii
rexmt_timeout 10 server 10.10.3.3
```

tftp This command initiates command mode TFTP service. Specify an IP address/name to directly access the client or issue the tftp command with your choice of ancillary values.

Alternatively, use [add tftp request](#) to configure the TFTP service and use [enable tftp request](#) to activate TFTP service.

Syntax

```
tftp <host name or IP address>
```

Table 64 TFTP Command Descriptions

Parameter	Description
ascii	Set text mode to ASCII. Default
binary	Set text mode to OCTET
connect [host_name]	Connect to the remote TFTP server
get [remotefile] [localfile]	Receive a file
help	Print help information
mode [ascii binary]	Set file transfer mode: ASCII or Binary
put [localfile] [remotefile]	Send a file
quit	Exit TFTP
rexmt	Set the retransmission timeout interval. The range is 1-60. The default is 5 seconds.

Table 64 TFTP Command Descriptions

Parameter	Description
status	Show current TFTP request status
timeout	Set maximum timeout interval. The range is 1-300. The default is 25 seconds.
trace	Toggle packet tracing
verbose	Toggle verbose mode echoes command
?	Print help information

Example

```
tftp 10.10.3.3
```

Related Commands

[add tftp request](#)

[enable tftp request](#)

4

REMOTE ACCESS COMMANDS

This chapter describes the following Remote Access Commands:

- [Network Dial-In Access](#)
- [Network Dial-Out Access: Dialout](#)
- [SLIP](#)

Network Dial-In Access

This section describes the commands you must use to provide remote access services to dial-in network users.

add ip pool

This command assigns a specified number of contiguous IP addresses for allocation by the router card. When dial-in network users are dynamically assigned IP addresses, those IP addresses are allocated from a pool which has the advantage of bundling several IP addresses into one to limit RIP advertisements.

The pool is created as a range, starting from an initial address/subnet mask. As PPP or SLIP users dial in, IP allocates an address from this pool and assigns them to the user. IP addresses are automatically allocated on a *public* or *private* basis for users who aren't assigned to a pool (public) or for those who are (private). Pools are also advertised as *aggregate*, *no_aggregate*, or *multiple_aggregate* routes. If an IP pool is configured as an *aggregate* address pool, the associated network route will get added to the Routing Table immediately, and be advertised as a *single* network route. If the address pool is defined as *no_aggregate*, individual host routes are added to the Routing Table when a user dials in and receives an address from the IP address pool. If the IP pool is specified as *multiple_aggregate*, the pool is divided into a number of routes, depending on the value entered for *max_unused_addrs*.

The router card automatically derives subnet masks for *aggregate* users but a mask can be configured for *no_aggregate* users.



Users assigned to more than one pool will receive an address from the last assigned pool in round robin fashion. Also, if the administrator reduces the size of the pool, users whose associated address pool was deleted won't be denied access until after their calls have terminated.

Syntax

```

add ip <pool name>
    initial_pool_address <IP address/subnet>
    advertise_type [always | inuse]
    max_unused_addrs <0 to 4096>
    route [aggregate | no_aggregate | multiple_aggregate]
    size <1 to 4096>
    state [public | private]
    priority <1 to 256>
    use_type [local | shared]

```

Table 65 Add IP Pool Command Parameter Descriptions

Parameter	Description	Settings	Default
pool name	Designation of the IP pool.	Up to 16 ASCII characters.	—
initial_pool_address/subnet_mask	First IP network address to be assigned from the specified pool, with or without a mask specifier. The mask specifier can be 'A', 'B', 'C', 'H', or a numeric value from 8 to 30 (32 for host) that describes the number of one bits in the mask. If you do not specify a mask, the router card will generate the natural netmask from the <i>initial_pool_address</i> .	xxx.xxx.xxx.xxx	—
advertise_type	The type of advertising used.	always never	—
max_unused_addrs	The maximum number of IP address that will be wasted (unused) when multiple aggregate IP routes are created. This field is only valid if route type is <i>multiple_aggregate</i> .	0 to 4096	—
route	Broadcasts the pool as a single network (aggregate), individual host routes (no_aggregate), or multiple networks (multiple_aggregate).	aggregate no_aggregate multiple_aggregate	no_aggregate
size	Number of allowable IP addresses. Class C values exceeding x.x.x.255 will increment to x.x.1.1.	1 to 4096	1
state	Type of pool created. A <i>public</i> pool allocates IP addresses to any caller not assigned a pool; a <i>private</i> pool is limited to specified users.	public private	public
priority	The priority in which the pool will assign IP addresses.	1 to 256	—
use_type	The type of use implemented.	local shared	—

Related Commands[add address_pool user](#)[delete address_pool user](#)[delete ip pool](#)[enable ip address_pool_filtering list ip pools](#)[set ip pool](#)

add mpip client This command creates an entry for the router card configured as an MPIP client, in the MPIP server's Client Table with a password shared by the configured client and server, and the type of client specified.

Syntax

```
add mpip client <IP address>
    sharedsecret <string>
    type [hiper | netserver]
```

Table 66 Add MPIP Client Command Parameter Descriptions

Parameter	Description	Settings	Default
<IP address>	The unique identifier of the MPIP client.	xxx.xxx.xxx.xxx	—
sharedsecret	Password shared by the MPIP client and server.	Up to 16 ASCII characters.	—
type	The product type of the MPIP client. The distinction between these types is relevant only to a router card configured as an MPIP server. NETServer-based MPIP clients must specify NETServer type.	hiper netserver	hiper

Example

```
add mpip client 10.10.3.3 sharedsecret psswrđ type hiper
```

Related Commands[delete mpip client](#)[list mpip clients](#)[set mpip client](#)

add mpip server This command creates an entry for the router card configured as an MPIP server, in the MPIP client's server table with a password shared by the configured client and server.

Syntax

```
add mpip server <IP address>
    port <number>
    priority <1 to 32>
    sharedsecret <string>
```

Table 67 Add MPIP Server Command Parameter Descriptions

Parameter	Description	Settings	Default
<IP address>	Unique identifier of the MPIP server.	xxx.xxx.xxx.xxx	—
port	The UDP port all the router card MPIP servers use.	0 to 65535	5912
priority	Rank specifying preference of MPIP server used. If two servers share the same priority, the server with the smaller IP address takes precedence.	1 to 32	1
sharedsecret	Password shared by MPIP server and client.	Up to 16 ASCII characters.	—

Related Commands

[delete mpip server](#)
[list mpip servers](#)
[set mpip server](#)

list ip aggregate_routes This command displays all routes that were configured using the [add ip pool](#) command, including the pool name, aggregate route, size, and type.

Syntax

```
list ip aggregate_routes
```

Example

```
list ip aggregate_routes
```

Related Commands

```
add ip pool
```

list mpip bundles This command displays bundle owners and users for the Multilink PPP links registered by MPIP clients. This command displays data only when the router card is acting as an MPIP server and when MPIP calls are up for a machine acting as a client.

Syntax

```
list mpip bundles
```

Example

```
list mpip bundles
```

list mpip clients This command displays IP addresses and client types (router card or NETServer) of all Multilink PPP clients you configured using the [add mpip client](#) command.

Syntax

```
list mpip clients
```

Example

```
list mpip clients
```

Related Commands

[add mpip client](#)

[delete mpip client](#)

[set mpip client](#)

list mpip links This command displays all Multilink PPP links registered by MPIP clients.

Syntax

```
list mpip links
```

Table 68 List MPIP Links Description

Parameter	Description
Bundle owner	IP address of the first client receiving any bundle on this link (where the link terminates).
Link Owner	IP address of the virtual client receiving a bundle first.
Link ID	Entry for each configured link.
User Name	The name of the user transmitting the bundle.

Example

```
list mpip links
```

list mpip locallinks This command displays MPIP client information, including all MPIP users and their respective bundle owners—the remote access server where MPIP links are terminated. The command displays an *index* entry in the table for each configured MPIP link, that link's *bundle owner* (first client receiving any bundle on this link), and *user* (name of the user sending the bundle).

Syntax

```
list mpip locallinks
```

Example

```
list mpip locallinks
```

list mpip servers This command displays all Multilink PPP servers you configured using the [add mpip server](#) command. The command lists the IP address, UDP port, and the priority.

Syntax

```
list mpip servers
```

Example

```
list mpip servers
```

Related Commands

[add mpip server](#)

[delete mpip server](#)

[set mpip server](#)

set connection This command configures global connection parameters for all dial-in users. Use the [show connection settings](#) command to display current settings.

Syntax

```
set connection
    banner_file <string>
    command_prompt <string>
    host_select [round_robin | random]
    manage_user_access [disabled | enabled]
    manage <manage | prompt>
    message <message string>
    service <dialin user prompt>
    user_name <user name>
    login_host_timeout <time>
    data_buffering [disabled | enabled]
```

```
ondemand_retries <0 to 500>
ondemand_retry_interval <0 to 600>
```

Table 69 Set Connection Command Parameter Descriptions

Parameter	Description	Settings	Default
banner_file	ASCII string that denotes the name of a text file that has been placed in the router card's file system using tftp. The contents of the banner file is used as the port banner. The maximum size of a banner file is 4096 bytes. Also refer to the <i>set modem_group</i> and <i>set switched interface</i> commands.	1 to 4096 (bytes)	—
command_prompt	ASCII string that will appear at the command prompt.	Up to 64 characters.	—
host_select	Specifies how the system chooses which host to connect the user to. Next host is chosen sequentially (round_robin) or randomly (random).	round_robin random	round_robin
manage_user_access	If disabled, any user with MANAGE permission set will be disconnected when attempting to dial in to the router card.	enabled disabled	enabled
manage	The string displayed when a dial-in user is connected and has become a <i>manage</i> user.	Up to 64 ASCII characters.	manage:
message	ASCII string defines a global connection message. If the interface has no message set this message is displayed when the user connects.	Up to 256 ASCII characters.	—
service	String that prompts the connected dial-in user who has both login and network access enabled.	Up to 64 ASCII characters.	Login/ Network User
user_name	String that serves as the user prompt. The global user name " <i>default</i> " is specified if no name is entered.	Up to 64 ASCII characters.	default
login_host_timeout	Time in seconds the router card is given to connect to one of the available login hosts. This allows host timeout to be tailored to the external network conditions and it provides a fast response for the user.	1 to 600	9
data_buffering	For a login user, specifies whether CIP to Telnet buffering is enabled or disabled.	enabled disabled	—
ondemand_retries	The number of on-demand retries.	0 to 500	—
ondemand_retry_interval	The interval in seconds between on-demand retries.	0 to 600	—

Example

```
set connection banner_file conn1 command_prompt >> host_select
round_robin manage_user_access disabled manage prompt user_name
bsmith data_buffering enabled ondemand_retries 100
ondemand_retry_interval 100
```

set ip pool This command modifies IP pool parameters set using the [add ip pool](#) command.

Syntax

```
set ip pool <pool name>
    initial_pool_address <IP_address/subnet>
    max_unused_addrs <0 to 4096>
    route [aggregate | no_aggregate | multiple_aggregate]
    size <1 to 4096>
    state [public | private]
    advertise_type [always | inuse]
    priority <0 to 256>
    use_type [local | shared]
```

Table 70 Set IP Pool Command Parameter Descriptions

Parameter	Description	Settings	Default
<pool name>	Designation of the IP pool.	Up to 16 characters.	—
initial_pool_address/subnet_mask	First IP address to be assigned from the specified pool, in the format nnn.nnn.nnn.nnn, with or without a mask specifier. The mask specifier can be 'A', 'B', 'C', 'H', or a numeric value from 8 to 30 (32 for host) that describes the number of one bits in the mask. If you do not specify a mask, the router card will generate the natural netmask from the <i>initial_pool_address</i> .	xxx.xxx.xxx.xxx	—
max_unused_addrs	This parameter specifies the maximum number of IP address that will be wasted (unused) when multiple aggregate IP routes are created. This field is only valid if route type is <i>multiple_aggregate</i> .	0 to 4096	—
route	Broadcasts the pool as a single network (aggregate), individual host routes (no_aggregate), or multiple networks (multiple_aggregate).	no_aggregate multiple_aggregate	no_aggregate
size	The number of allowable IP addresses. Class C values exceeding x.x.x.255 will increment to x.x.1.1.	1 to 4096	1
state	Type of pool created. A <i>public</i> pool allocates IP addresses to any caller not assigned a pool; a <i>private</i> pool is limited to specified users.	public private	public

Table 70 Set IP Pool Command Parameter Descriptions

Parameter	Description	Settings	Default
advertise_type	The type of advertising used.	always inuse	—
priority	The priority in which the pool will assign IP addresses.	1 to 256	—
use_type	Type of use.	local shared	—

Related Commands[add address_pool user](#)[add ip pool](#)[delete address_pool user](#)[delete ip pool](#)[enable ip address_pool_filtering](#)[list ip pools](#)

set ipx system This command sets parameters for dynamic IPX networks. The maximum number of hops allowed is 15.

Syntax

```
set ipx system
  default_gateway <IPX host address>
  initial_pool_address <IPX network address>
  max_hops <number>
  name <string>
  number <internal network number>
  pool_members <number>
  ppp_users_network_address <ipx_address>
  priority <number>
```

Table 71 Set IPX System Command Parameter Descriptions

Parameter	Description	Settings
default_gateway	The default router for the dynamic IPX network. Command settings are xxxxxxxx.xx:xx:xx:xx:xx:xx where the xxxxxxxx is an IPX Network Address and the xx:xx:xx:xx:xx:xx is a MAC address.	xxxxxx xx.xx:xx:xx:xx: xx:xx
initial_pool_address	First IPX address used to dynamically assign IPX network.	xxxxxxx Values of ffffffff or ffffffff are invalid.
max_hops	The maximum number of hops this network will make to locate an IPX system.	1 to 64
name	Designation for the dynamic IPX network.	Up to 256 ASCII characters.
number	Network address for the dynamic IPX network. This value is required to run various IPX services. See add ipx service command for more information.	xxxxxxx Values of ffffffff or ffffffff are invalid.
pool_members	Number of addresses to reserve in the pool of IPX addresses used when dynamically assigning IPX networks.	1 to 4096
ppp_users_network_address	Unique IPX network address assigned to unnumbered PPP dial-in users only if they are configured through the set network user <name> ipx command with the address fffffffc.	xxxxxxx Values of ffffffff or ffffffff are invalid.
priority	Preference for the dynamic IPX network.	1 to 3

set ppp This command sets global parameters for PPP which apply to all calls, including the call type for which PPP compression will be attempted/accepted. Issuing this command overrides the *compression algorithm* parameter set by the [set network user <user name> ppp](#) command.



Users who dial in and receive a compressed_analog connection (MNP5 or V.42bis) won't receive PPP compression. Payload compression is set by the parameter—not header compression as set for a user.

Syntax

```
set ppp
    authentication_preference [chap | default | eap | ms_chap |
    pap | radius_eap_proxy]
    bap_hunt_group_phone_number <phone number>
    ccp_modemtype_accept [none | all, digital, compressed_analog,
    uncompressed_analog]
    dns_usage [system | ppp | client | none]
    nbns_primary <IP address>
    nbns_secondary <IP address>
    pppdns_primary <IP nbns address>
    pppdns_secondary <IP nbns address>
    receive_authentication [none | pap | chap | any | eap |
    ms_chap | any_except_mschap | encrypted_any |
    radius_eap_proxy]
    session_start_message <string>
    system_mtu <128 to 1518>
    pap_retries <1 to 10>
    dns_usage [system | ppp | client | none]
```

Table 72 Set PPP Command Parameter Descriptions

Parameter	Description
authentication _preference	If the <i>receive authentication</i> value is set to ANY, this value will set the authentication type for the <i>first</i> attempt. If the Default setting is selected, authentication types will be negotiated in this order of preference: CHAP, EAP, MS_chap and PAP. This value works in conjunction with <i>receive_authentication</i>
bap_hunt_group _phone_number	The phone number for the Band Width Allocation Protocol (BAP) hunt group.
ccp_modemtype _accept	The call type for which PPP compression will be attempted/accepted. Issuing this command overrides the <i>compression algorithm</i> parameter set by the set network user <name> ppp command. <ul style="list-style-type: none"> ■ None—No PPP data compression for any call type. ■ All—PPP data compression will always be attempted. ■ Digital—PPP data compression only for digital calls. Default. ■ Compressed_analog—PPP data compression only for compressed (modem compression) analog calls. ■ Uncompressed_analog—PPP data compression only for uncompressed (modem compression) analog calls. Default. ■ Pppoe—If the interface is PPOE, then compression is negotiated depending on the value of a private ppp variable.
dns_usage	Enables/disables the router card to supply clients with Domain Name System (DNS) server addresses used in IPCP negotiation. Options are client, none, ppp, or system.
nbns_primary	IP address of the primary NetBIOS name server
nbns_secondary	IP address of the secondary NetBIOS name server
pppdns_primary	The Domain Name Server (DNS) primary server address used in IPCP negotiation. This will be used only if there is no user-specific value available.
pppdns_ secondary	The Domain Name Server (DNS) secondary server address used in IPCP negotiation. This will be used only if there is no user-specific value available.
system _mtu	System Maximum Transmission Unit. Values are between 128 and 1518.
pap_retries	The number of retries between 1 and 10.
dns_usage	DNS usage: system, PPP, Client, or None.

set mpip This command configures MPIP port numbers and on/off status for any router card acting as a MPIP server or client. Setting this command does not affect the MPIP Server and MPIP Client tables.

Syntax

```
set mpip
    server_state [off | on]
    client_state [off | on]
    port <number>
```

Table 73 Set MPIP Command Parameter Descriptions

Parameter	Description	Settings	Default
server_state	Turns all MPIP servers on or off.	on	off
		off	
client_state	Turns all MPIP clients on or off.	on	on
		off	
port	The UDP port for the MPIP server and client.	0 to 65535	5912

Example

```
set mpip server_state on client_state on port 9000
```

Related Commands

[show mpip settings](#)

set mpip client This command configures MPIP client parameters you set with the [add mpip client](#) command.

Syntax

```
set mpip client <IP address>
    sharedsecret <string>
    type [hiperarc | netserver]
```

Table 74 Set MPIP Client Command Parameter Descriptions

Parameter	Description	Settings	Default
<IP address>	Unique identifier of the MPIP client.	xxx.xxx.xxx.xxx	—
sharedsecret	Password shared by the MPIP client and server.	Up to 16 ASCII characters.	—
type	The product type of the MPIP client: the access router card or NETServer. The distinction between types is relevant only to a router card configured as an MPIP server—NETServer-based MPIP clients must specify NETServer type.	hiperarc netserver	hiperarc

Example

```
set mpip client 10.10.3.3 sharedsecret psswrđ type hiperarc
```

Related Commands

[add mpip client](#)

[delete mpip client](#)

[list mpip clients](#)

set mpip server This command configures MPIP server parameters you set with the [add mpip server](#) command.

Syntax

```
set mpip server <IP_address>
    port <number>
    priority <1-32>
    sharedsecret <string>
```

Table 75 Set MPIP Server Command Parameter Descriptions

Parameter	Description	Settings	Default
<IP address>	Unique identifier of the MPIP server.	xxx.xxx.xxx.xxx	—
port	The UDP port all the router card MPIP servers use.	0 to 65535	5912
priority	Rank specifying preference of MPIP server used. If two servers share the same priority, the server with the smaller IP address takes precedence.	1 to 32	1
sharedsecret	Password shared by the MPIP client and server.	Up to 16 ASCII characters.	—

Example

```
set mpip server 10.10.3.3 port 5913 priority 2 sharedsecret psswrđ
```

Related Commands

[add mpip_server](#)

[delete mpip_server](#)

[list mpip_servers](#)

show mpip settings This command displays MPIP server configuration set with [set mpip_server](#).

Syntax

```
show mpip settings
```

Example

```
show mpip settings
```

NTP

This section contains commands for enabling, disabling, setting, and altering the Network Time Protocol (NTP) system settings.

disable ntp This command disables the Simple NTP which references clocks located on the Internet.

Syntax

```
disable ntp
```

Example

```
disable ntp
```

Related Commands

[enable ntp](#)

[set ntp](#)

enable ntp This command enables the NTP, which references a clock located on the Internet, allowing the router card to synchronize its clock setting with a server of your choice.

Syntax

```
enable ntp
```

Example

```
enable ntp
```

Related Commands

[set ntp](#)

[disable ntp](#)

set ntp This command controls the NTP settings used by the access router card, and sets parameters for the NTP client process, which references a clock located on the Internet. This is useful to specify the server you want the router card to access for time synchronization. Support for NTP is based on RFC 2030, using Unicast mode only. See the [show ntp settings](#) command to display ntp configuration

Syntax

```
set ntp
    polling_interval <64 to 1024>
    primary_server <host name or IP address>
    retransmissions <0 to 200>
    secondary_server <host name or IP address>
    timeout <1 to 60>
```

Table 76 Set NTP Command Parameter Descriptions

Parameter	Description	Settings	Default
polling_interval	Period in seconds the NTP process takes to gather time synchronization information.	64 to 1024	600
primary_server	IP address or host name of the server the router card will contact first for time synchronization.	xxx.xxx.xxx.xxx	—
retransmissions	The maximum number of times a request is retransmitted to a specified server before the server is considered unavailable.	1 to 200	5
secondary_server	IP address or host name of the server the router card will contact for time synchronization whenever the primary server is unavailable.	xxx.xxx.xxx.xxx	—
timeout	Number of seconds since a request has been sent to a server, after which period the request is considered timed-out.	1 to 60	10

Example

```
set ntp polling_interval 1000 primary_server 10.10.3.3
retransmissions 10 secondary_server 10.10.3.4 timeout 30
```

Related Commands

[show ntp settings](#)

show ntp settings This command displays Simple Network Time Protocol settings.

Syntax

```
show ntp settings
```

Example

```
show ntp settings
```

Related Commands

[set ntp](#)

Network Dial-Out Access: Dialout

dial This command generates an outgoing call to the location specified by the user name. You can use the list users command to list the defined users, along with the services they are defined to work with, and their current status. The limit is 64 ASCII characters.

Syntax

```
dial <user name>
```

Example

```
dial user2
```

Related Commands

[list users](#)

dialout l2tp This command generates a dial-out call to a specified remote user (similar to the manual dial-up call) and brings up an L2TP tunnel.

Syntax

```
dialout l2tp <user name>
```

Example

```
dialout l2tp user2
```

dialout pptp This command generates a dial-out call to a specified remote user (similar to a manual dialup call) and brings up an PPTP tunnel.

Syntax

```
dialout pptp <user_name>
```

Example

```
dialout pptp user2
```

set dialout user This command sets a local IP address for the dialout user to use with the session and also automates the dialout connection.

Syntax

```
set dialout user <username>
    local_ip_address <IP address>
    reply1_script <string>
    reply2_script <string>
    reply3_script <string>
    reply4_script <string>
    reply5_script <string>
    reply6_script <string>
    send1_script <string>
    send2_script <string>
    send3_script <string>
    send4_script <string>
    send5_script <string>
    send6_script <string>
```

The **send_x_script** and **reply_x_script** parameters are strings that are sent to the remote system and replies expected back from the remote system. If a dialout user does not have a phone number set, the router card automatically uses the commands set in send scripts to perform the dialout. The send scripts must include the modem dialing commands and phone number.

The maximum size of a **send_x_script** or **reply_x_script** parameter is 240 characters. The string must be enclosed in double quotes (" ") if it exceeds 64 characters.

The escape character (\) can be inside the quoted string. If the escape character \ is followed by b, f, n, r, t or v it inserts special characters in the string as follows:

- \b = backspace
- \f = formfeed
- \n = newline
- \r = carriage return
- \t = tab
- \v = vertical tab

If the escape character (\) is followed by an x the next two characters are interpreted as a hexadecimal constant. \x0A = 0x0a.

If the escape character (\) is followed by any other character that character is placed in the token.

A double quote on either side of a special character places it in the token. For example; "\"" places a \ in the string.

The **send1_script** is sent first, then the router card waits for a message back that matches the **reply1_script** and so on.

Example

The following command line sets up the dialout user george to dial out to the phone number 555-2222 and login as the user ppp with a password of ppp43.

```
set dialout user george send1_script "at\r" reply1_script "OK"
send2_script "atdt5552222\r" reply2_script "login:"
send3_script "ppp43\r" reply3_script "password:" send4_script
"ppp43\r"
```

Modem Groups

add modem_group This command creates a group of interfaces. Also see the set modem_group command, which configures all interfaces in the modem group. You can also add additional interfaces to this modem group using assign interface, and remove them with unassign interfaces. Modem groups *all* and *slot:1/mod:[1-y]*, *slot:2/mod:[1-y]*, etc. are provided as default modem groups with associated Hub modems as indicated. Use list modem_groups command to view entries.



Modem groups are a shorthand notation for a list of interfaces. They do not hold interface configuration settings. Default modem groups cannot be modified.

Syntax

```
add modem_group <group name>
    interfaces [slot:x/mod:[1-y], slot:x/mod:[1-y]...]
```

Table 77 Add Modem_Group Command Parameter Descriptions

Parameter	Description
<group_name>	Name of the modem group. We recommend you limit the length of this name to eight characters. That will ensure the name will always display completely in certain list and show commands. The limit is 64 ASCII characters. The limit is 500 modem groups.
interfaces	List of interfaces to be assigned to the modem group. The expected format is ssss,ssss,ssss... where the Interface Name must exist in the Interface Table. Interface names can be individual names, or ranges. A range must be in the format slot:x/mod:[1-y],slot:x/mod:[1-y].

Related Commands

[delete_modem_group](#)
[disable_modem_group](#)
[enable_modem_group](#)
[hangup_modem_group](#)
[list_modem_groups](#)
[set_modem_group](#)
[show_modem_group](#)

assign interfaces This command adds interfaces to an existing modem group or modem groups. To display interfaces assigned to a modem group, use the [show_modem_group](#) command. Modem groups are added by the [add_modem_group](#) command and displayed by the [list_modem_groups](#) command.

Syntax

```
assign interfaces <slot:x/mod:[1-y], slot:x/mod:[1-y],...>
    modem_group <group_name>
```

Table 78 Assign Interfaces Command Parameter Descriptions

Parameter	Description
interface name	Interfaces to be assigned to the modem group. The Interface Name must exist in the Interface Table. Interface names can be individual names or ranges. A range must be in the format slot:x/mod:[1-y]; for example: slot:3/mod [2-4], slot:5/mod:6. The limit is 64 ASCII characters.
modem_group	Name of the modem group.

Example

```
assign interfaces slot:3/mod:2, slot:5/mod:6
```

Related Commands

[show modem_group](#)

[add modem_group](#)

[list modem_groups](#)

delete modem_group

This command removes a modem group from the Modem Group Table. You can list current modem groups and their assigned interfaces using the [list modem_groups](#), and [show modem_group](#) commands.



Default modem groups such as `al, slot:1/mod:[1-y]` and others can not be modified or deleted.

Syntax

```
delete modem_group <group_name>
```

Example

```
delete modem_group mdmgrp2
```

Related Commands

[add modem_group](#)

[disable modem_group](#)

[enable modem_group](#)

[hangup modem_group](#)

[list modem_groups](#)

[set modem_group](#)

[show modem_group](#)

disable modem_group

This command disables the modem group you enabled with the [enable modem_group](#) command. Modem groups `all` and others incorporating installed modem cards (e.g.: `slot:3`) are provided as default modem groups, making system-wide or slot-by-slot disabling possible. Use the [show modem_group](#) command to view INACTIVE status of disabled modem groups.

Syntax

```
disable modem_group <name>
```

Example

```
disable modem_group mdmgrp2
```

Related Commands

[add_modem_group](#)
[delete_modem_group](#)
[enable_modem_group](#)
[hangup_modem_group](#)
[list_modem_groups](#)
[set_modem_group](#)

list modem_groups This command displays modem groups that you previously defined using the [add_modem_group](#) command, along with the number of ports in each group. This command also lists default modem groups for each slot and all ports (all).

Syntax

```
list modem_groups
```

Example

```
list modem_groups
```

Related Commands

[add_modem_group](#)
[delete_modem_group](#)
[disable_modem_group](#)
[enable_modem_group](#)
[hangup_modem_group](#)
[set_modem_group](#)
[show_modem_group](#)

show modem_group This command displays the switched interfaces that belong to the specified modem group and their status.

Syntax

```
show modem_group <name>
```

Example

```
show modem_group mdm3
```

Related Commands

[add_modem_group](#)
[delete_modem_group](#)
[disable_modem_group](#)
[enable_modem_group](#)
[hangup_modem_group](#)
[list_modem_groups](#)
[set_modem_group](#)

Network Service

add network service This command configures a network listener process that provides certain services, including modem sharing, TFTP file access, and SNMP, Telnet and ClearTCP support. To view the available server types, use the list available servers command.

Syntax

```

add network service <service_name>
    close_active_connections [true | false]
    data <ancillary data options>
    enabled [yes | no]
    server_type [cleartcpd | snmpd | tftpd | telnetd | rshd]
    socket <socket_number>

```

Table 79 Add Network Service Command Parameter Descriptions

Parameter	Description
<service_name>	Name of this type of service. The limit is 32 ASCII characters.
close_active_connections	Indicates whether or not to close any active connections when a service is disabled by the disable network_service command. The default is False.
data	Ancillary Data. This field contains server-specific configuration data. See table below for configurable ancillary data values for Telnet. The <i>modem_group</i> value also applies to NCSI DialOut service.

Table 79 Add Network Service Command Parameter Descriptions

Parameter	Description
enabled	<i>Optional.</i> Indicates whether the network is enabled (YES) or disabled (NO). When you add a network service, it is <i>enabled</i> by default.
server_type	Designates the type of service being offered. Services currently available are: <ul style="list-style-type: none"> ■ ClearTCPD - Daemon enables access to a modem group. Uses TCP. ■ SNMPD - Daemon supports SNMP. Uses UDP. ■ TFTPD - Daemon supports file transfer service. Uses UDP. ■ TELNETD - Daemon supports Telnet, either to the CLI or a modem group. Uses TCP. ■ RSHD - Daemon supports RSH and RCP. Uses UDP.
socket	Port the server listens on. For TFTP, Telnet and CLEARTCP, it is the TCP or UDP port number. Socket numbers are the joined sender's (or receiver's) IP address and service type's port number. The maximum is 65535. The range is 0 to 65535.

The following table shows configurable values for network service, which are specified with the **data** parameter.

Table 80 Data Parameter Descriptions

Ancillary Data Value	Description
auth	On indicates that login/password authentication should be performed on incoming connections. Feature not supported for DialOut service. Format: auth= [on off] The default is on.
drop_on_hangup	Value specifying whether the TCP session is dropped after modem hangs up. <i>Off</i> allows connection to remain active. Feature not supported for DialOut service. The default is off.
login_banner	ASCII string sent to a client when connection is made. It must be quoted and offset by backslashes if spaces are included in the string. Specify carriage return after login banner with login_banner=string\r\n. This Feature is not supported for DialOut service. The format is login_banner=string The default is none.

Table 80 Data Parameter Descriptions

Ancillary Data Value	Description
login_prompt	<p>ASCII string specifying the login prompt sent during authentication. It must be quoted and offset by backslashes if spaces are included in the string. Feature not supported for Dial-Out service. Specify a carriage return after the login banner with login_banner=string\r\n\.</p> <p>The format is login_prompt=string</p> <p>The default is login:.</p>
modem_group	<p>ASCII string specifying the name of a modem group for whose modems network service is supplied. This value must be specified when using DialOut service.</p>
service_type	<p>Indicates whether the service offered is modem sharing or manage.</p> <p><i>Modem sharing</i> service connects a client to <i>multiple</i> modems.</p> <p><i>Manage</i> service connects a client to the <i>command line</i>, to manage the system. Applicable only to Telnet servers; you can't use ClearTCP to access the system for management.</p> <p>Format: service_type=manage, dialout</p> <p>The default is manage.</p>

Examples

To configure a ClearTCP service to offer modem sharing on TCP port 6000, without authentication upon connect, using the modem slot:3/mod:1, enter:

```
add network service modem_sharing server_type cleartcpd socket
6000 data auth=off,interface=slot:3/mod:1,service_type=dialout
```



Enclose DATA values including spaces with double quotes. E.g.: data modem_group="Hi Boston".



CAUTION: Do not create more than one Dial-Out service with the same name on a network.

To configure a Telnet service to offer CLI access on port 6666, doing authentication upon connect (default) and dropping the connection on hangup, enter:

```
add network service CLI_access server_type telnetd socket 6666
data drop_on_hangup=on
```

To configure a Dial-Out service using the modem group LA, enter:

```
add network service "Calling LA" server_type dialout data
modem_group=LA
```

Related Commands

[delete network service](#)

[disable network service](#)

[enable network service](#)

[list network services](#)

[set network service](#)

list network services This command displays all network services you defined using the add network service command.

Syntax

```
list network services
```

- **Name**—name of service. Values displayed are TELNET (*default*), TFTP (*default*), DialOut, SNMP, or ClearTCP.
- **Server Type**—type of network server. For example, TFTP (TFTP daemon).
- **Socket**—TCP port number used (you assign or by default) by the service.
- **Close**—reveals whether all connections close when you disable this service. TRUE or FALSE. See add network service command for details.
- **Admin Status**—the status you have requested for this service. Enabled or disabled. See the add network service command for details.

Example

```
list network services
```

Related Commands

[add network service](#)

[delete network service](#)

[disable network service](#)

[enable network service](#)

[set network service](#)

set network service This command sets parameters for network services you configured with the [add network service](#) command. You can list the configured network services using [list network services](#). Service must first be *disabled* for this command to work. For dialout service, the only Data value supported is *modem_group* (and this value must be used when implementing DialOut service).

Syntax

```
set network service <admin name>
    close_active_connections [true | false]
    data <string>
    server_type [cleartcpd | snmpd | tftpd | telnetd]
    socket <socket_number>
```

Table 81 Set Network Service Command Parameter Descriptions

Parameter	Description
<admin_name>	Designation you assigned to network service with the add network service command. The limit is 64 ASCII characters.
close_active_connections	Indicates whether or not to close any active connections when a service is shut by disable network_service. The default is False.
data	TELNET and ClearTCP Ancillary Data. This field contains server-specific configuration data. See table which lists the configurable ancillary data parameters in the add network service command.
server_type	Type of network service you wish to assign to this administration name. Available services: <ul style="list-style-type: none"> ■ ClearTCPD—daemon enables access to a modem group on socket 0. Uses TCP. ■ SNMPD—daemon supports SNMP on socket 161. Uses UDP. ■ TFTPD—daemon supports file transfer service on socket 69. Uses UDP. ■ TELNETD—daemon supports TELNET, either to the CLI or a modem group on socket 23. Uses TCP.
socket	The port the server listens on. For TFTP, TELNET and ClearTCP, it is the TCP or UDP port number. Socket numbers are the joined sender's (or receiver's) IP address and service type's port number. The range is 0-65535.

Related Commands

[add network service](#)
[delete network service](#)
[disable network service](#)
[enable network service](#)
[list network services](#)

delete network service This command deletes the specified network service from the list of available services. You must use [disable network service](#) before deleting the service. You can see which services are available and active using the [list available servers](#) and [list network services](#) commands.

Syntax

```
delete network service <service name>
```

Example

```
delete network service tftpd
```

Related Commands

[add network service](#)

[disable network service](#)

[enable network service](#)

[set network service](#)

disable network service This command disables a network service, such as telnet or TFTP. If *close_active_connection* was specified as TRUE in the [add network service](#) command, then all active connections are closed when the service is disabled.

Syntax

```
disable network service <service name>
```

Example

```
disable network service tftpd
```

Related Commands

[add network service](#)

[delete network service](#)

[enable network service](#)

[list network services](#)

[set network service](#)

enable network service This command enables the network service that you previously defined with the [add network service](#) command. You can see which services are currently defined and their state using [list network services](#).

Syntax

```
enable network service <service name>
```

Example

```
enable network service tftpd
```

Related Commands

[add network service](#)

[delete network service](#)

[disable network service](#)

[list network services](#)

[set network service](#)

list available servers This command displays the available network servers and supported network services. The choices are RSHD service, SNMP service, telnet service, TFTP service, or ClearTCP. The services listed by this command are used in the *server_type* field of the [add network service](#) command.

Syntax

```
list available servers
```

Example

```
list available servers
```

Related Commands

[add network service](#)

SLIP

disable slip offloading This command disallows gateway card from trying to offload SLIP framing to modem cards. Use the [show slip](#) command to view edits.

Syntax

```
disable slip offloading
```

Example

```
disable slip offloading
```

Related Commands

[show slip](#)

[enable slip offloading](#)

enable slip offloading This command allows gateway card to try offloading SLIP framing to modem cards. Use the show slip command to view edits. The default is enabled.

Syntax

```
enable slip offloading
```

Example

```
enable slip offloading
```

Related Commands

```
disable slip offloading
```

set slip session_start_message This command is used to modify the session start message sent to dialin slip users, a message string to display at a client's terminal when a connection is established and SLIP is begun in the router card.

Syntax

```
set slip session_start_message <string>
```

The limit is 256 ASCII characters. You can add additional values as follows:

- **%server_ip**—identification of the router card's local (server's) IP address.
- **%client_ip**—identification of remote (client's) IP address.

If the string is surrounded by double quotes, you can insert an escape character '\ ' inside the quoted string. If the string is followed by the characters **b, f, n, r, t** or **v**, the router card will place special characters in the string, as follows:

- **\b** = backspace
- **\f** = formfeed
- **\n** = newline
- **\r** = carriage return
- **\t** = tab
- **\v** = vertical tab

If the string is followed by an **x**, the next two characters will be interpreted as a hexadecimal constant as follows:

- **x0A** = 0x0a

If the string is followed by *any other character*, that character will be placed in the token.

Other rules state the following:

- A double quote (") will place the double quote in the token
- A forward slash '/' will place one forward slash in the token

Example

```
set slip session "SLIP session beginning now from%server_ip
to%client_ip."
```

show slip settings This command displays SLIP configurations. When enabled, it indicates that SLIP framing can be off-loaded to the modem card (if the modem card is capable of doing it) and the *start message*, which appears when the SLIP connection comes up. The default is enabled.

Syntax

```
show slip settings
```

Example

```
show slip settings
```

Related Commands

```
set slip session_start_message
```

Cross Connect Commands

add cross_connect This command adds a cross connect.

Syntax

```
add cross_connect <name>
    peak <0 to 65535>
    vci1 <32 to 65535>
    vci2 <32 to 65535>
    vpi1 <0 to 255>
    vpi2 <0 to 255>
```

Example

```
add cross_connect cc2 peak 100 vci1 200 vci2 250 vpi1 110 vpi2 160
```

Related Commands

[delete cross_connect](#)

[enable cross_connect](#)

[show cross_connect](#)

[list cross_connect](#)

delete cross_connect This command deletes a cross connect.

Syntax

```
delete cross_connect <name>
```

Example

```
delete cross_connect cc2
```

Related Commands

[add cross_connect](#)

[enable cross_connect](#)

[show cross_connect](#)

[list cross_connect](#)

enable cross_connect This command enables cross connect after it has been added.

Syntax

```
enable cross_connect <name>
```

Example

```
enable cross_connect cc2
```

Related Commands

[add cross_connect](#)

[delete cross_connect](#)

[show cross_connect](#)

[list cross_connect](#)

show cross_connect This command shows cross connection settings.

Syntax

```
show cross_connect <name>
```

Example

```
show cross_connect <name>
```

Related Commands

[add cross_connect](#)

[delete cross_connect](#)

[enable cross_connect](#)

[list cross_connect](#)

list cross_connect This command lists current cross connections.

Syntax

```
list cross_connect
```

Example

```
list cross_connect
```

Related Commands

[add cross_connect](#)

[delete cross_connect](#)

[enable cross_connect](#)

[show cross_connect](#)

5

INTERFACE AND MODEM COMMANDS

This chapter describes Interface and Modem Commands in the following sections:

- [DS1 Interface](#)
- [Modem Auto-Answer Commands](#)
- [TAP](#)
- [RS232](#)
- [TAP](#)

DS1 Interface

assign interfaces This command adds interfaces to an existing modem group or modem groups. To display interfaces assigned to the modem group, use the show modem_group command. Modem groups are added by the add modem_group command and displayed by the list modem_groups command.

Syntax

```
assign interfaces <slot:x/mod:[1-y], slot:x/mod:[1-y],...>  
modem_group <group_name>
```

Example

```
assign interfaces slot5:/mod:1 modem_group mdmgrp3
```

add logical_ds1 interface This command is used to add a logical T1/E1 Interface. This command is used in conjunction with the [set logical_ds1 interface](#) command, which is used to determine the number of T1/E1 channels to allocate for the logical interface.

Syntax

```
add logical_ds1 interface <logical_interface_name>
```

Related Commands

[delete logical_ds1 interface](#)

[set logical_ds1 interface](#)

[show logical_ds1 interface <logical_interface_name> ch_map](#)

delete logical_ds1 interface

This command is used to delete a logical T1/E1 Interface.

Syntax

```
delete logical_ds1 interface <logical_interface_name>
```

Related Commands

[add logical_ds1 interface](#)

[set logical_ds1 interface](#)

[show logical_ds1 interface <logical_interface_name> ch_map](#)

disable interface

This command disables any specified interface. If a call is up on the interface it is disconnected. A disabled interface remains in the Interface Table, but does not transmit or receive any data. Enter multiple interfaces as follows: slot:2/mod:5,slot:2/mod:7,slot:4/mod:3,slot:4/mod:8, or a range: slot:1/mod:[1-9]. Use the [list interfaces](#) command to see the currently defined interfaces, and their status.

Syntax

```
disable interface <interface name>
```

Example

```
disable interface slot:2/mod:5,slot:2/mod:7
```

Related Commands

[enable interface](#)

[set interface](#)

[show interface <interface name> settings](#)

enable interface

This command enables the specified interface. Enabling an interface enables it to transmit and receive data. You can enter multiple interfaces (ssss,ssss,ssss) or a range (slot:3/mod:[1-96]). You can use [list interfaces](#) to see which interfaces are defined, and whether they are currently disabled. Use the [show icmp settings](#) command to view edits.

Syntax

```
enable interface <interface_name>
```

Example

```
enable interface slot:2/mod:5
```

Related Commands

[disable interface](#)

[set interface](#)

[show icmp settings](#)

[show interface <interface name> settings](#)

hangup interface This command disconnects any calls (causes the connection on the specified interface to hangup and leave the interface(s) in an *enabled* state. You can enter multiple interfaces in the form slot:1/mod:4,slot:2/mod:3 or a range: slot:1/mod:[1-96].

Syntax

```
hangup interface <interface_name>
```

Example

```
hangup interface slot:2/mod:5
```

list active interfaces This command displays the operational status, administration status and name of all active interfaces. The output is the same as that from the list interfaces command, except non-active interfaces are not displayed. Inactive interfaces are interfaces with no current connections. Operational status indicates current operating state of the interface, UP or DOWN. Administrative status indicates the permanently configured status of the interface, UP or DOWN. For modem interfaces, Oper Status will be down only if you disable the modem

Syntax

```
list active interfaces
```

Example

```
list active interfaces
```

list ds_one interfaces This command displays list of DS1 interfaces.

Syntax

```
list ds_one interfaces
```

Example

```
list ds_one interfaces
```

list connections This command displays all connections established on switched interfaces, listing the following information:

Syntax

```
list connections
```

The following information is displayed:

- **IfName**—Modem slot and interface of current connections.
- **User Name**—Name of users currently connected.
- **Type**—Current type of connections established on modems. They include:
 - **On-demand**—User connection established for on-demand purposes.
 - **Dial-back**—User connection established for callback purposes.
 - **Continuous**—User connection established for continuous utilization.
 - **Manual**—User connection established on the fly.
 - **Timed**—User connection established for a particular interval.
 - **ShrMod (Shared-modem)**—Dial-out user connection to a modem utilizing a login service (Telnet or rlogin) or NCSI. LED does not light until call is unhooked (amber) and connected (green). NCSI sessions using the port redirector display *None* as the DLL type.
 - **Dialin**—User connection established for dial-in purposes. LED lights *amber* when modem is unhooked, *green* when call is connected.
 - **Bond**—User connection utilizing bandwidth allocation.
 - **Dedicated**—User connection established for a particular user.
 - **VOIP**—User connection for voice calls.
- **DLL**—Data link layer that the specified dial-in session is connected to: NONE, PPP, SLIP, SHELL, RL(O)G(I)N, TLNT, PING, ADMN, CL(EAR)TCP, L2TP, PPTP, TAP, PRMT, G.711, G.729.
- **Start Date**—Start date of a connection established on the specified interface.
- **Start Time**—Start time of a connection established on the specified interface.

Example

```
list connections
```

list interfaces This command displays the installed interfaces, along with their operational status and administration status. If an interface is down under Admin Status, you can use `enable interface` to try to bring it up. This command also identifies the Frame Relay logical name—a representation of the Frame Relay PVC instance - in order to add an IP or IPX network on top of the PVC.

Syntax

```
list interfaces
```

Table 82 List Interface Description

Parameter	Description
Interface Name	LAN interface name such as eth:1 or eth:2, or ATM interfaces such as ds3:1, atmaal:1 and atmcell:1.
Oper Status	Current operating status of the interface, Up or Down. For modem interfaces, Oper Status will be Down only if the modem is disabled.
Admin Status	Permanently configured status of the interface, Up or Down.

Example

```
list interfaces
```

list ip interface_block This command displays the IP addresses associated with each system interface. If the interface has a point-to-point connection, then the neighbor field contains the address of the remote system. This command lists:

Syntax

```
list ip interface_block
```

Table 83 List IP Interface_block Description

Parameter	Description
Address	IP address of the router card interface.
Neighbor	IP address of the remote system.
Status	Status of the connection: enabled or disabled.
Interface	Any valid interface.

Example

```
list ip interface_block
```

list switched interfaces This command displays the installed switched interfaces (modems), along with their operational and administration status. If an interface is down under Admin Status, you can use enable interface to try to bring it up. The command lists:

Syntax

```
list switched interfaces
```

Table 84 List Switched Interface Description

Parameter	Description
Interface Name	Interface name. For example, slot:3/mod:1
Oper Status	Current operating state of the interface; Up or Down. Oper Status is Up only if modem is connected.
Admin Status	State of the interface configured by the administrator. Values displayed is either Up or Down.

Example

```
list switched interfaces
```

list sync interfaces This command lists all of the V35 Interfaces.

Syntax

```
list sync interfaces
```

Example

```
list sync interfaces
```

Related Commands

[set sync interface](#)

[show sync interface](#)

set ds1 interface This command is used to configure a T1/E1 Interface and to enable detection of alarms.

Syntax

```
set ds1 interface <physical_interface_name>
    ais_evt [trap | disable_all | log | enable_all]
    cablelen [to131ft | to262ft | to393ft | to524ft | to655ft |
to789ft | longhaul]
    clocksource [looptiming | localtiming]
    linecode [b8zs | hdb3 | ami]
    linebuildout [db0 | db7_5 | db15 | db22_5]
    linetype [esf | d4 | e1 | e1crc | e1mf | e1crcmf]
    loopback_evt [trap | disable_all | log | enable_all]
    los_evt [trap | disable_all | log | enable_all]
    rcvtestcode_evt [trap | disable_all | log | enable_all]
    red_evt [trap | disable_all | log | enable_all]
    sndais_evt [trap | disable_all | log | enable_all]
    sndyellow_evt [trap | disable_all | log | enable_all]
    yellow_evt [trap | disable_all | log | enable_all]
```

Table 85 Set DS1 Interface Command Parameters Descriptions

Parameter	Description
ais_evt	Enables the generation of an SNMP trap for Far End Sending Alarm Indication Signal conditions on this interface. Valid values are trap, disable_all, log, enable_all. The default is enable_all.
cablelen	For T1 only. Ignored for E1. Indicates the length of cable. Valid values are to131ft, to262ft, to393ft, to524ft, to655ft, to789ft, longhaul. The default is to131ft.
clocksource	Sets the source of the transmit clock. Valid values are: <ul style="list-style-type: none"> ■ localtiming - local clock source is used as the transmit clock ■ looptiming - recovered receive clock is used as the transmit clock The default is looptiming.
linebuildout	This parameter is for T1 spans configured for longhaul. Ignored for E1. Line Buildout allows the WAN interface to compensate for internal or external Digital Service Unit/Control Service Units (DSU/CSUs). For internal DSU/CSUs, the WAN interface must compensate for the decibel level. For external DSU/CSUs, the WAN interface must compensate for the length of the cable that connects the T1/E1 NIC to the DSU/CSU. Valid values are: <ul style="list-style-type: none"> db0 — 0 decibels db7_5 — -7.5 decibels db15 — -15 decibels db22_5 — -22.5 decibels The default is db0.

Table 85 Set DS1 Interface Command Parameters Descriptions (continued)

Parameter	Description
linecode	Sets the type of Zero Code Suppression used on the line. Valid values are: <ul style="list-style-type: none"> ■ ami—Alternate Mark Inversion (T1 and E1) ■ b8zs—Bipolar 8 Zero Substitution (T1 and E1) ■ hdb3—High Density Bipolar 3 (E1 only) The default is b8zs.
linetype	Sets the type of framing used on the line. Valid values are: <ul style="list-style-type: none"> ■ d4—AT&T D4 Format DS1 (T1 only) ■ esf—Extended SuperFrame DS1 (T1 only) ■ e1—CCITT Recommendation G.704 (Table 4a) (E1 only) ■ e1crc—CCITT Recommendation G.704 (Table 4b) (E1 only) ■ e1crcmf—G.704 (Table 4b) with TS16 multiframing enabled (E1 only) ■ e1mf—G.704 (Table 4a) with TS16 multiframing enabled (E1 only) The default is esf.
loopback_evt	Enables the generation of an SNMP trap for Near End Loopback conditions on this interface. Valid values are trap, disable_all, log, enable_all. The default is enable_all.
los_evt	Enables the generation of an SNMP trap for Near End Loss Of Signal conditions on this interface. Valid values are trap, disable_all, log, enable_all. The default is enable_all.
rcvtestcode_evt	Enables the generation of an SNMP trap for Near End Test Code conditions on this interface. Valid values are trap, disable_all, log, enable_all. The default is enable_all.
red_evt	Enables the generation of an SNMP trap for Near End Loss Of Frame (in red alarm condition) conditions on this interface. Valid values are trap, disable_all, log, enable_all. The default is enable_all.
sndais_evt	Enables the generation of an SNMP trap for Near End Sending Alarm Indication Signal conditions on this interface. Valid values are trap, disable_all, log, enable_all. The default is enable_all.
sndyellow_evt	Enables the generation of an SNMP trap for Near End Sending Yellow Alarm conditions on this interface. Valid values are trap, disable_all, log, enable_all. The default is enable_all.
yellow_evt	Enables the generation of an SNMP trap for Far End Loss of Frame conditions (signaled by a received Yellow Alarm) on this interface. Valid values are trap, disable_all, log, enable_all. The default is enable_all.

set logical_ds1 interface

This command is used to assign channels (DS0s) on a fractional T1/E1 interface to a logical T1/E1 interface that is created using the [add logical ds1 interface](#). A 1.544 Mbps T1 line is partitioned into twenty four 64 Kbps channels which can be grouped to create a logical interface whose bandwidth matches your requirements. A 2.048 E1 line is the European equivalent of the T1 line and is partitioned into thirty one 68 Kbps channels that you can group.

Syntax

```
set logical_ds1 interface <logical_interface_name> ch_map
<ds_timeslots>
```

Table 86 Set Logical DS1 Interface Command Parameters Descriptions

Parameter	Description
logical_interface_name	Logical T1/E1 interface comprised of one or more fractional T1/E1 channels, or DS0s. A logical T1/E1 interface uses the following naming convention. wan: <number>-<linkname>. For example, wan:1-boston.
ds_timeslots	List or range of DS0s assigned to a logical_ds1 interface. For example you can specify the range using the following formats: 1,2,3,4 or 1-4 or 1-4,6,8-10

Related Commands

[add logical_ds1 interface](#)

[delete logical_ds1 interface](#)

[show logical_ds1 interface <logical_interface_name> ch_map](#)

show ds1 interface

This command displays information for a physical T1/E1 interface.

Syntax

```
show ds1 interface <physical_interface_name>
```

The following information is displayed.

- **NIC Type**—Type of network interface card
- **Line Type**—Type of framing used on the line
- **Line Code**—Type of Zero Code Suppression used on the line
- **Transmit Clock Source**—Source of the transmit clock
- **Cable Length**—Cable length setting
- **Line Buildout**—Type of line buildout used to compensate for internal or external Digital Service Unit/Control Service Units (DSU/CSUs)
- **Yellow Alarm Evt**—Setting for SNMP trap generation for Far End Loss of Frame conditions
- **Snd Yellow Alarm Evt**—Setting for SNMP trap generation for Near Ending Sending Yellow Alarm conditions

- **Alarm Ind Sig Evt**—Setting for SNMP trap generation for Far End Sending Alarm Indication Signal conditions
- **Snd Alarm Ind Sig Evt**—Setting for SNMP trap generation for Near End Sending Alarm Indication Signal conditions
- **Red Alarm Evt**—Setting for SNMP trap generation for Near End Loss of Frame (in red alarm condition) conditions
- **Loss of Sig Evt**—Setting for SNMP trap generation for Near End Loss of Signal conditions
- **Loopback Evt**—Setting for SNMP trap generation for Near End Loopback conditions
- **Rcv Test Code Evt**—Setting for SNMP trap generation for Near End Test Code conditions

set switched interface

This command configures port parameters for the specified switched (modem) interface (slot:2/mod:1, e.g.). To display switched interfaces you have configured, use the [list switched interfaces](#) command. To view settings for a particular interface, use the [show interface <interface name> settings](#) command.



*When setting connection type, be aware that the `direct_net` parameter does **not** support the SLIP protocol. `Direct_net` requires the use of a negotiated protocol, which SLIP is not.*

Syntax

```
set switched interface <interface name>
    access [dial_in | dial_out | two_way]
    at_command <string>
    call_type [l2tp | none | pptp]
    character_mode [even_seven_bit|no_parity_eight_bit|
    odd_seven_bit]
    connection_type [direct_conn | normal | direct_net | no_prompt
    | ppp_only | prompt_user_only]
    dial_prefix <string>
    disable_authentication [none | async_ppp | sync_ppp | ppp]
    dnis_authentication [disable | preferred | required]
    dnis_auth_time [before_answer | after_connect]
    dnis_auth_type [dnis | ani]
    dnis_password <ascii string>
    dnis_timeout <seconds>
    filter_access [on | off]
    host_address <IP_name or address>
```

```

host_type [prompt | select | specified]
init_script <name>
input_filter <name>
login_service [telnet | rlogin | cleartcp | ping]
message <login_string>
output_filter <name>
password <user_password>
password_prompt <prompt_message>
ppp_echo_request <0 to 5000>
prompt <prompt_message>
prompt_style [local | remote]
prompt_delay <seconds>
prompt_timeout <5 to 600>
protocol [ppp | slip]
special_xon_xoff_flow [disabled | enabled]
tcp_port <port_number>
type [network | login | login_network]
use_dnis_auth_pool [ enabled | disabled | required ]
user_name <user name>

```

Table 87 Set Switched Interface Parameter Descriptions

Parameter	Description
<interface_name>	The switched interface (slot:x/mod:y) to modify. The limit is 64 ASCII characters.
access	Sets access type for switched interface. The modem can allow dial-in only, dial-out only or both (TWO-WAY). The default is Two-way.
at_command	String representing any generic AT command. When implemented, output is shown immediately on CLI.
call_type	Sets the interface to expect a tunneling protocol. l2tp—set the expected tunneling protocol to L2TP none—no tunneling protocol expected. This is the default. pptp—set the expected tunneling protocol to PPTP.
character_mode	Set the character mode for an interface. Options: even_seven_bit—Seven bit, even parity. no_parity_eight_bit—Eight bit, no parity. Default. odd_seven_bit—seven bit odd parity.

Table 87 Set Switched Interface Parameter Descriptions (continued)

Parameter	Description
connection_type	<p>Sets connection type for switched interface. Options:</p> <ul style="list-style-type: none"> ■ Direct_net—Uses the protocol parameter's setting to create a network (virtual node) connection. Employs <i>user name</i> and <i>password</i> specified in this command. Authentication is done by the network protocol such as PPP. Direct_net <i>does not support</i> the SLIP protocol. ■ Direct_conn—Employs <i>user name</i> and <i>password</i> specified in this command to establish a login type connection to the target host. Authentication is accomplished by the target host. If user name and password are not specified with this choice, user "<i>default</i>" is employed. ■ Normal—Prompts for both <i>user name</i> and <i>password</i>. Default ■ Ppp_only—Configures a switched interface for PPP only. After an incoming call is connected, PPP is started immediately. There is no prompting for login, and no default user authentication. If the peer does not respond to any of the LCP configuration request packets, the link is disconnected. Authentication is done using the negotiated PPP authentication. ■ Prompt_user_only—Prompts for <i>user name</i> only and authenticate with the <i>password</i> specified in this command. ■ No_prompt—Does not prompt. Authenticates with the <i>user name</i> and <i>password</i> specified in this command. If user name and password are not specified with this choice, user "<i>default</i>" is employed.
dial_prefix	<p>Prefix added to all phone numbers dialing from this port. The limit is 7 characters.</p>
disable_authentication	<p>Sets enabling/disabling of authentication for types of dial-in users on a <i>per interface</i> basis. If authentication is disabled and a PPP call is auto-detected, the interface to which the user has dialed in will be checked for a configured user name which must previously have been entered using the <i>user_name</i> parameter in the above command. If <i>user_name</i> is specified for the particular interface, all user profile information will be forwarded without authentication. If no <i>user_name</i> is configured on the specified interface, <i>default</i> user's profile will be forwarded without authentication. The types of calls you can specify to disable authentication for are:</p> <ul style="list-style-type: none"> ■ None—Authentication is <i>not</i> disabled for any type of PPP call. Default ■ Async_ppp—Authentication is disabled if the incoming call is autodetected as a PPP <i>asynchronous</i> call ■ Sync_ppp—Authentication is disabled if the incoming call is autodetected as a PPP <i>synchronous</i> call. ■ PPP—Authentication is disabled if the incoming call is autodetected as a PPP call <p><i>Note:</i> When used, this feature disables all other types of authentication included local, RADIUS and TACACS+ authentication. The default is None.</p>
dnis_authentication	<p>Specifies how to perform DNIS authentication. Options:</p> <p>disabled—No DNIS authentication is performed.</p> <p>preferred—If the incoming call has the required phone number information (ANI or DNIS), then DNIS authentication is attempted.</p> <p>required—If the incoming call does not have the required phone number information (ANI or DNIS), then the call is dropped. If the incoming call has the required phone number information (ANI or DNIS), DNIS authentication is attempted.</p>

Table 87 Set Switched Interface Parameter Descriptions (continued)

Parameter	Description
dnis_auth_time	Specifies when DNIS authentication is performed. Options: before_answer—Perform DNIS authentication before answering. Default after_connect—Perform DNIS authentication after connection is made.
dnis_auth_type	Specify which phone number will be used as user-name attribute. Options: dnis—Use the DNIS phone number. ani—Use the ANI phone number.
dnis_password	An ASCII string to be used as the user-password attribute. The limit is 64 ASCII characters. The default is Empty string.
dnis_timeout	Number of seconds to wait for DNIS authentication. The range is 0-60. A value of 0 disables this feature. The default value is 0.
filter_access	Turns filtering ON or OFF. The default is Off.
host_address	IP address to connect a dial-in user to, if the host type is specified, and connection_type is direct_conn or direct_net.
host_type	Identifies how connection is established. Dial-in user is: <ul style="list-style-type: none"> ■ Prompt—prompted to enter a host name or address. ■ Select—connected to a login host, selected from the list of login hosts, determined by the host_select field in the <i>set connection</i> command. Default ■ Specified—connected to the configured IP address.
init_script	Name of modem initialization script used. Maximum size: 7 ASCII characters. If you are setting an init_script for a Modem Pool or Interface the init_script name must already exist. A null string ("") indicates the name will be deleted. The default is USR_int.
input_filter	File name of filter screening incoming data.
login_service	Login service to use if the connection_type is <i>not</i> direct_net. Options: <ul style="list-style-type: none"> ■ TELNET—<i>Default</i> ■ RLOGIN ■ ClearTCP ■ Ping—user pings a login host, receives a successful/unsuccessful message and is disconnected.

Table 87 Set Switched Interface Parameter Descriptions (continued)

Parameter	Description
message	<p>The string to display to a dial-in user when a connection is set. The limit is 64 ASCII characters.</p> <p>Use the following values to display system information in the message line:</p> <ul style="list-style-type: none"> ■ \$date—current date according to system uptime ■ \$callid—user’s call identification according to system uptime ■ \$port—port occupied by user (slot:x/mod:y) ■ \$hostname—user’s host name ■ \$sysname—user’s system name (same as hostname) ■ \$time—time of call according to system uptime <p>Message information may also be defined in a banner file. To specify the banner file which contains the message text use the following command line syntax:</p> <p>Set switched interface <slot:x/mod:y> message <banner_file name></p> <p>If the message text includes spaces it <i>must</i> be enclosed in double quotations. Use the show user command to view the message as configured.</p> <p>See the set connection command for more information.</p>
output_filter	File name of filter screening outgoing data.
password_prompt	String to present the dial-in user. The default is login. The limit is 64 ASCII characters.
ppp_echo_request	Range: 0 to 5000
prompt	String to present the dial-in user. The default is login. The limit is 64 ASCII characters.
prompt_style	Specifies whether prompting of the username and password on this interface will be provided by the router card (Local), or by a distant security service such as RADIUS or TACACS+ (remote). The default is Local.
prompt_delay	<p>The numbers of seconds to wait for a user to log in. Default is 0.</p> <p>Note: In most cases, you should use the default value of 0. If a value other than zero is used, and no successful user login has occurred within the specified time, the router card automatically logs the user in as the local user default using the default user’s settings <i>without authentication</i>.</p>
prompt_timeout	The maximum idle timeout for the username/password prompt for a dial-in connection. The default value is 5 minutes (300 seconds). If the prompt is idle for this time, the session will be terminated.
password	Used if connection_type is no_prompt or prompt_user_only. The limit is 63 ASCII characters. In order for any user to pass the authentication, this password configured for the user must match this switched interface. Also see set user password.
protocol	Protocol (PPP) to connect with, if connection type is direct_net. SLIP is not supported by <i>direct_net</i> connection type. The default is PPP.

Table 87 Set Switched Interface Parameter Descriptions (continued)

Parameter	Description
special_xon_xoff_flow	<p>Disables/enables the special XON/XOFF flow control in the router card for terminal application for Dialup lines. When a XOFF character sent by a client reaches the router card, the router card should stop transmitting data to the modem. Once the router card receives XON, it should resume the data transfer.</p> <p>The default is disabled. Only the terminal services (such as TELNET, CLEAR TCP dialin/dialout) will be affected by this configuration.</p> <p>For local users, use the following command to configure this feature: set user <name> special_xon_xoff_flow [disabled enabled]</p> <p>For RADIUS users, USR Vendor Specific Attribute 0x9879 configures this special flow control feature.</p> <p>Values 0 or Not Present - Disabled 1- Enabled</p>
tcp_port	TCP port number for login host. Value used for <i>direct_conn</i> or <i>direct_net</i> connection types. The limit is 65535.
type	<p>Type of connections to allow on the switched interface.</p> <ul style="list-style-type: none"> ■ Login port allows login users only ■ Network port allows network users only ■ Login_network allows either type. Default
use_dnis_auth_pool	Enables or disables the dnis authorization pool.
user_name	Designation for the switched interface, used if connection type is <i>no_prompt</i> . The limit is 64 ASCII characters.

set sync interface This command is used to configure a V35 interface.



*The parameter **flagidlepattern** has precedence over **idlepattern**. For example; When **flagidlepattern** is set to a value of **invalid** the value of **idlepattern** is picked up.*

Syntax

```
set sync interface <physical_if_name>
    clockinverted [none | clockinverted]
    clockreference [dtelookback | dcelookback]
    encoding [nrz | nrzi]
    flagidlepattern [yes | invalid]
    flowtype [none | ctsrts | dsrdtr]
    idlepattern [mark | space]
    minflags [1 | 2]
    rtscontrol [controlled | constant]
    rtsctsdelay <number>
    speed [bps64k | bps256k | bps1544k | bps2m | bps4m | bps8m]
```

Table 88 Set Sync Interface Command Parameter Descriptions

Parameter	Description
clockinverted	<p>Sets clock inverted mode for this interface. Valid values are none and clockinverted. The default is none.</p> <p>This parameter determines if data is internally latched at the rising or falling edge of the clock signal. Selecting clockinverted results in data being latched at the falling edge of the clock signal. When set to the default, none, data is latched at the rising edge of the clock signal.</p>
clockreference	<p>Sets clock reference mode for this interface. Valid values are dtloopback and dceloopback. The default is dtloopback.</p> <p>The following diagrams illustrate the differences between dtloopback and dceloopback:</p> <div style="text-align: center;"> <p>DTE Loopback Normal Mode (CISCO)</p> </div> <div style="text-align: center;"> <p>DCE Loopback Mode</p> </div>
encoding	<p>Sets the bit stream encoding technique used for this port. Valid values are:</p> <ul style="list-style-type: none"> ■ nrz—Non-Return to Zero encoding ■ nrzi—Non-Return to Zero Inverted encoding <p>The default is nrz.</p>
flagidlepattern	Sets the flag idle pattern value. Valid settings are yes and invalid. The default is yes.
flowtype	<p>Sets the type of flow control used on this interface. Valid values are:</p> <ul style="list-style-type: none"> ■ none—No flow control. ■ ctsrts—Use ctsRts flow control. ■ dsrdtr—Use dsrDtr flow control. <p>The default is ctsrts.</p>
idlepattern	Sets the bit pattern used to indicate an idle line. Valid values are mark and space. The default is space.

Table 88 Set Sync Interface Command Parameter Descriptions (continued)

Parameter	Description
minflags	Sets the minimum number of flag patterns this interface needs to recognize the end of one frame and the start of the next. Valid values are 1 and 2. The default is 2.
rtscontrol	Sets the method used to control the Request to Send (RTS) signal. Valid values are: <ul style="list-style-type: none"> ■ controlled—DTE asserts RTS each time data needs to be transmitted and drops RTS at some point after data transmission begins. ■ constant—DTE constantly asserts RTS. The default is constant.
rtsctsdelay	Sets the interval (in milliseconds) that DCE must wait, after it sees RTS asserted, before asserting CTS. The range is 0 to 65535. The default is 0.
speed	Sets the line speed for this interface. Valid values are bps64k, bps256k, bps1544m, bps2m, bps4m, and bps8m. The default is bps2m. Make sure that you set the speed value correctly. In the dceloopback mode the speed value is used to determine the clock frequency on pin 113.

show bootrom ip interface

This command displays the following IP boot configurations for the Ethernet interface (*eth:1* or *eth:2*).

Syntax

```
show bootrom ip interface <eth:x>
```

- IP Address
- IP Gateway
- TFTP Server
- IP Netmask
- TFTP Download
- Load File Name
- Crashdump File Name

Example

```
show bootrom ip interface eth:1
```

```
show ds1 interface  
<physical_interface_  
name> ch_map
```



This command displays the channels, or DS0s assigned to a logical T1 or E1 interface.

The Access field displays unallocated channels.

Syntax

```
show ds1 interface <physical_interface_name> ch_map
```

Example

If channels 1 through 6 are assigned to an interface called wan:1-ch(icago), and channels 7 through 12 are assigned to wan:1-ny, this command displays:

```
wan:1-ch Channel Map: 1 2 3 4 5 6
```

```
wan:1-ny Channel Map: 7 8 9 10 11 12
```

```
access:
```

Related Commands

[add_logical_ds1_interface](#)

[set_logical_ds1_interface](#)

show ds1 interface
<physical_interface_
name> current_tbl

This command displays the T1/E1 Near End configuration information. It lists the following information:

Syntax

```
show ds1 interface <physical_interface_name> current_tbl
```

- Time Elapsed (Secs)—The number of seconds that have elapsed since the beginning of the current error-measurement period.
- Valid Intervals—Number of previous intervals (up to 96) for which valid data was collected.
- Line Status—This is an integer representing the Line Status as a bit map. Each bit indicates if a particular condition is present.
 - Far end LOF (Yellow Alarm)—Indicates Far End Loss of Frame condition (signaled by a received Yellow Alarm) on this interface.
 - Near end sending LOF Indication—Indicates Near End Sending Loss of Frame Indication condition (sending Yellow Alarm) on this interface.
 - Far end sending AIS—Indicates Far End Sending Alarm Indication Signal condition on this interface.
 - Near end sending AIS—Indicates Near End Sending Alarm Indication Signal condition on this interface.
 - Near end LOF (Red Alarm)—Indicates Near End Loss of Frame condition (in red alarm) on this interface.
 - Near end Loss Of Signal—Indicates Near End Loss of Signal condition on this interface.
 - Near end is looped—Indicates Near End Loopback conditions on this interface.
 - E1 TS16 AIS—Indicates Alarm Indication Signal received condition on an E1 link (signaled by a 1s pattern in time slot 16).
 - Far End Sending TS16 LOMF—Indicates For E1, a Loss of Multiframe Failure condition, diagnosed from bad multiframe alignment signals in time slot 16
 - Near End Sending TS16 LOMF—Near End sending a time slot 16 Loss of Multiframe Failure condition.
 - Near End detects a test code—Near End detects a test code condition
 - Other Failure—None of the above
- Current ESs—Number of errored seconds in the current 15-minute interval
- Current SESs—Number of Severely Errored Seconds in the current 15-minute interval
- Current SEFs—Number of Severely Errored Framing Seconds in the current 15-minute interval
- Current UASs—Number of Unavailable Seconds in the current 15-minute interval

- Current CSSs—Number of Controlled Slip Seconds in the current 15-minute interval
 - Current PCVs—Total number of Path Coding Violations in the current 15-minute interval
 - Current LESs—Number of Line Errored Seconds in the current 15-minute interval
 - Current BESs—Number of Bursty Errored Seconds in the current 15-minute interval
 - Current DMs—Number of Degraded Minutes in the current 15-minute interval
- Current LCVs—Total number of Line Code Violations in the current 15-minute interval

show ds1 interface
<physical_interface_
name>
fend_current_tbl

This command displays T1/E1 Far End Current Table.

Syntax

```
show ds1 interface <physical_interface_name> fend_current_tbl
```

- Time Elapsed (Secs)—The number of seconds that have elapsed since the beginning of the current error-measurement period
 - Valid Intervals—Number of previous intervals (up to 96) for which valid data was collected
 - Current ESs—Number of errored seconds in the current 15-minute interval
 - Current SESs—Number of Severely Errored Seconds in the current 15-minute interval
 - Current SEFs—Number of Severely Errored Framing Seconds in the current 15-minute interval
 - Current UASs—Number of Unavailable Seconds in the current 15-minute interval
 - Current CSSs—Number of Controlled Slip Seconds in the current 15-minute interval
 - Current LESs—Number of Line Errored Seconds in the current 15-minute interval
 - Current PCVs—Total number of Path Coding Violations in the current 15-minute interval
 - Current BESs—Number of Bursty Errored Seconds in the current 15-minute interval
- Current DMs—Number of Degraded Minutes in the current 15-minute interval

show ds1 interface
<physical_interface_
name>
fend_interval_tbl

This command displays T1/E1 Far End Interval Table.

Syntax

`show ds1 interface <physical_interface_name> fend_interval_tbl`

- Intvl—A number between 1 and 96, where 1 is the most recently completed 15 minute interval and 96 is the least recently completed 15 minutes interval (assuming that all 96 intervals are valid)
- ESs—Number of errored seconds in the period indicated by “Intvl” parameter
- SESs—Number of Severely Errored Seconds in the period indicated by “Intvl” parameter
- SEFs—Number of Severely Errored Framing Seconds in the period indicated by “Intvl” parameter
- UASs—Number of Unavailable Seconds in the period indicated by “Intvl” parameter
- CSSs—Number of Controlled Slip Seconds in the period indicated by “Intvl” parameter
- PCVs—Total number of Path Coding Violations in the period indicated by “Intvl” parameter
- LESs—Number of Line Errored Seconds in the period indicated by “Intvl” parameter
- BESs—Number of Bursty Errored Seconds in the period indicated by “Intvl” parameter
- DMs—Number of Degraded Minutes in the period indicated by “Intvl” parameter
- LCVs—Total number of Line Code Violations in the period indicated by “Intvl” parameter

show ds1 interface
<physical_interface_
name> fend_total_tbl

This command displays T1/E1 Far End Total Table.

Syntax

`show ds1 interface <physical_interface_name> fend_total_tbl`

- Total ESs—Number of errored seconds in the previous 24-hour interval
- Total SESs—Number of Severely Errored Seconds in the previous 24-hour interval
- Total SEFs—Number of Severely Errored Framing Seconds in the previous 24-hour interval
- Total UASs—Number of Unavailable Seconds in the previous 24-hour interval
- Total CSSs—Number of Controlled Slip Seconds in the previous 24-hour interval
- Total LESs—Number of Line Errored Seconds in the previous 24-hour interval

- Total PCVs—Total number of Path Coding Violations in the previous 24-hour interval
- Total BESs—Number of Bursty Errored Seconds in the previous 24-hour interval
- Total DMs—Number of Degraded Minutes in the previous 24-hour interval

show ds1 interface
<physical_interface_
name> interval_tbl

This command displays T1/E1 Near End Interval Table.

Syntax

```
show ds1 interface <physical_interface_name> interval_tbl
```

- Intvl—A number between 1 and 96, where 1 is the most recently completed 15 minute interval and 96 is the least recently completed 15 minutes interval (assuming that all 96 intervals are valid)
- ESs—Number of errored seconds in the period indicated by “Intvl” parameter
- SESs—Number of Severely Errored Seconds in the period indicated by “Intvl” parameter
- SEFSs—Number of Severely Errored Framing Seconds in the period indicated by “Intvl” parameter
- UASs—Number of Unavailable Seconds in the period indicated by “Intvl” parameter
- CSSs—Number of Controlled Slip Seconds in the period indicated by “Intvl” parameter
- PCVs—Total number of Path Coding Violations in the period indicated by “Intvl” parameter
- LESs—Number of Line Errored Seconds in the period indicated by “Intvl” parameter
- BESs—Number of Bursty Errored Seconds in the period indicated by “Intvl” parameter
- DMs—Number of Degraded Minutes in the period indicated by “Intvl” parameter
- LCVs—Total number of Line Code Violations in the period indicated by “Intvl” parameter

show ds1 interface
<physical_interface_
name> total_tbl

This command displays T1/E1 Near End Total Table.

Syntax

```
show ds1 interface <physical_interface_name> total_tbl
```

- Total ESs—Number of errored seconds in the previous 24-hour interval
- Total SESs—Number of Severely Errored Seconds in the previous 24-hour interval
- Total SEFs—Number of Severely Errored Framing Seconds in the previous 24-hour interval
- Total UASs—Number of Unavailable Seconds in the previous 24-hour interval
- Total CSSs—Number of Controlled Slip Seconds in the previous 24-hour interval
- Total PCVs—Total number of Path Coding Violations in the previous 24-hour interval
- Total LESs—Number of Line Errored Seconds in the previous 24-hour interval
- Total BESs—Number of Bursty Errored Seconds in the previous 24-hour interval
- Total DMs—Number of Degraded Minutes in the previous 24-hour interval
- Total LCVs—Total number of Line Code Violations in the previous 24-hour interval

show interface
<interface name>
settings

This command displays settings for the specified modem or Ethernet interface.

Syntax

```
show interface <interface name> settings
```

- **Description**—Name of the interface driver. Ethernet, ATM or Modem drivers.
- **Type**—Kind of physical serial interface. For example: RS232 or Ethernet-CSMA/CD.
- **Speed**—Estimate of the interface's current bandwidth in bits per second.
- **High Speed**—Estimate of the interface's current bandwidth in units of 1,000,000 bits per second, exceeding 20 million bits/second.
- **Administrative Status**—Permanently configured state of the interface. Choices: Up or Down.
- **Operational Status**—Current state of the interface. Choices: Up or Down.
- **Link Up/Down Traps**—Permanently configured value indicating whether linkUp/linkDown traps should be generated for this interface. Choices: enabled (default) or disabled.

- **Promiscuous Mode**—When set to FALSE (default), this interface accepts packets/frames addressed only to this station. When set to TRUE, the station accepts all packets/frames transmitted on the network.
- **Connector Present**—When set to TRUE (default) the interface sublayer has a physical connector and FALSE (default) when otherwise.
- **Filter Access**—This switch allows user filters to override the specified interface filter. If set to OFF (default), user filters do not override the interface filters. If set to ON, user filters override the interface filter.
- **Last Change**—Last configuration change made to the interface, measured in system time.
- **Input Filter**—Name of the input filter enabled for the specified interface.
- **Output Filter**—Name of the output enabled filter for the specified interface.
- **Physical address**—MAC address of the specified Ethernet interface.
- **Host Type**—The type of host this dial-in user is currently connected to. Choices: PROMPT, SELECT and SPECIFIED. The default is SELECT.
- **Connection Type**—Kind of connection this interface is configured for. Choices: DIRECT_CONN, NORMAL, DIRECT_NET, NO_PROMPT, and PROMPT_USER_ONLY. The default is NORMAL.
- **Port Type**—The type of physical port configured. Choices: NETWORK, LOGIN and LOGIN_NETWORK (default)
- **User Name**—Name of connected user. This value is set only if the port is configured not to prompt for user name.
- **Access**—Direction of calls currently configured on this interface. Choices: DIAL_IN, DIAL_OUT or TWO_WAY (default).
- **Dial Prefix**—A number defining the prefix to the phone number.
- **Init Script**—Initialization script currently in use. The default is USR_int.
- **TCP Port**—TCP port number you associate with the login service. The default is 0. The range is 0 to 65535.
- **Protocol**—Currently connected protocol type. Choices: PPP or SLIP. The default is PPP.
- **Prompt**—Dial-in prompt you set for this interface. The limit is 64 ASCII characters.
- **Prompt Style**—Specifies whether prompting of the username and password on this interface is provided by the router card (LOCAL), or by a distant security service - TACACS+ (REMOTE). The default is LOCAL.
- **Message**—Salutation you specified for this interface. The limit is 64 ASCII characters.
- **Host address**—IP address of the host specified for this interface.
- **Disable Authentication for call type**—The type of call for which authentication will be disabled

- **Login Service**—Type of login service you configured for this interface.
- **Call Type**—The type of tunneling protocol expected on a call
- **DNIS Authentication**—Specifies how to perform DNIS authentication. disabled—No DNIS authentication is performed. preferred—If the incoming call has the required phone number information (ANI or DNIS), then DNIS authentication is attempted. required—If the incoming call does not have the required phone number information (ANI or DNIS), then the call is dropped. If the incoming call has the required phone number information (ANI or DNIS), DNIS authentication is attempted.
- **DNIS Authentication Time**—Specifies when DNIS authentication is performed. before_answer—Perform DNIS authentication before answering. before answer is the default. after_connect—Perform DNIS authentication after connection is made.
- **DNIS Authentication Type**—Specify which phone number will be used as user-name attribute. dnis—Use the DNIS phone number. ani—Use the ANI phone number.
- **Character Mode**—The character mode for transmitting and receiving information
- **DNIS Authentication Timeout**—Number of seconds to wait for DNIS authentication. The range is 0-60. A value of 0 disables this feature. The default value is 0.
- **Prompt Delay**—The numbers of seconds to wait for a user to log in.
- **Authentication**—Indication of whether dial-in user's profile is forwarded with (enabled) or without (DISABLED) authentication. The default is enabled.
- **Login Service**—Login service to use if the connection_type is not direct_net

Related Commands

[disable link_traps interface](#)

[enable modem_group](#)

```
show logical_ds1
  interface
<logical_interface_
  name> ch_map
```

This command displays the channel assignments for a logical T1/E1 Interface.

Syntax

```
show logical_ds1 interface <logical_interface_name> ch_map
```

Related Commands

[add logical_ds1 interface](#)

[delete logical_ds1 interface](#)

[set logical_ds1 interface](#)

unassign interface
<interface_name_list>
modem_group
<group_name>

This command removes the specified interface from the list of interfaces previously assigned to the specified modem group.

Syntax

```
unassign interface <interface_name_list> modem_group <group_name>
```

Related Commands

[assign interfaces](#)

[delete modem_group](#)

[disable modem_group](#)

[enable modem_group](#)

[list modem_groups](#)

[set modem_group](#)

[show modem_group](#)

Call Reject Code Commands

enable call reject_code

When enabled, the access router card supplies a reject code to the DSP Multispan card, which is then forwarded to the switch.

Syntax

```
enable call reject_code
```

Example

```
enable call reject_code
```

Related Commands

[disable call reject_code](#)

[show call reject_code status](#)

disable call reject_code

When disabled the access router card does not supply a reject code to the DSP Multispan card, and the DSP fills in a reject code as it deems appropriate.

Syntax

```
disable call reject_code
```

Example

```
disable call reject_code
```

Related Commands

[enable call reject_code](#)

[show call reject_code status](#)

show call reject_code status This command shows the status of the call reject code. Status is enabled or disabled.

Syntax

```
show call reject_code status
```

Example

```
show call reject_code status
```

Related Commands

[enable call reject_code](#)

[disable call reject_code](#)

Modem Auto-Answer Commands

disable auto_answer This command disables auto answering of modem-sharing-dial-out calls, for example; telnet or CTCP dial-out calls.

Syntax

```
disable auto_answer
```

Example

```
disable auto_answer
```

Related Commands

[enable auto_answer](#)

[show auto_answer](#)

enable auto_answer This command enables auto answering of modem-sharing-dial-out calls, for example; telnet or CTCP dial-out calls.

Syntax

```
enable auto_answer
```

Example

```
enable auto_answer
```

Related Commands

[disable auto_answer](#)

[show auto_answer](#)

show auto_answer This command displays the setting (enabled or disabled) for auto_answer.

Syntax

```
show auto_answer
```

Example

```
show auto_answer
```

Related Commands

[disable auto_answer](#)

[enable auto_answer](#)

Modem Chassis Slot Commands

set chassis slot This command configures a specific type of NAC modem card, the ownership of the slot, the number of ports to be enabled on a card in a slot, and the type of entry for that slot. The default card_type parameter is EMPTY.

Syntax

```
set chassis slot <number>

card_type <quad_modem | quad_i_modem | hdm_24 | hdm_30 |
jhdm_t1 | jhdm_e1 | jhdm_e1_r2_up | jhdm_e1_up | jhdm_t1_up |
sdh_nac_card | ds3_card | empty>

console [yes | no]

span <1 to 4>

owner [yes | no]

type <static>

ports <1 to 31>
```

Table 89 Set Chassis Slot Command Parameters Descriptions

Parameter	Description
slot number	Slot number in chassis from 1-16. Slot numbers can be specified in a range, such as: 4, 7, 8-14
console	When set to yes, the console of the HDM in the indicated slot becomes accessible. As with other ports, this is required if there is no network management card in the chassis and user has to do static configuration of cards.
span	Span number in the card from 1 to 4.
owner	Specifies the ownership of a particular slot. Ownership means the router card communicates with modem interfaces resident on a card in this slot. Ownership is required because there may be more than one router card within the same chassis. Modem cards in the chassis must be partitioned among the various router cards within the chassis so that packet bus sessions from each modem can be established with the corresponding router card. The default is yes.

Table 89 Set Chassis Slot Command Parameters Descriptions (continued)

Parameter	Description
type	Changes the row type to <i>static</i> so chassis configuration data learned from the network management card chassis message may be saved to the configuration file. When chassis configuration entries are created after receiving a chassis awareness message from the network management card, the row type is set to <i>dynamic</i> . Any entries created through a CFM load, SNMP set, or CLI command render the row type <i>static</i> . Only static entries are saved to the configuration file via CFM.
card_type	Type of card hardware in the slot. They include: <ul style="list-style-type: none"> ■ QUAD_MODEM—V.34-type modem card (1-4 ports) ■ QUAD_I_MODEM—ISDN-type modem card (1-4 ports) ■ HDM_24—24-channel DSP Single Span card (1-24 ports) ■ HDM_30—30-channel DSP Single Span card (1-30 ports) ■ JHDM_E1—DSP Multispan card (1-630 ports) ■ JHDM_T1—DSP Multispan card (1-651 ports) ■ JHDM_E1R2_UP ■ EMPTY—No card in slot. Number of ports set to zero. ■ DS3_CARD—DS3 card ■ SDH_NAC_CARD—SDH (synchronous digital hierarchy) card
ports	Sets the number of active ports for the card in the specified slot. The range is 1 to 31.

set chassis slot
<slot_list> console [no |
yes]

When set to yes, the console of the HDM in the indicated slot becomes accessible. As with other ports, this is required if there is no network management card in the chassis and user has to do static configuration of cards.

Syntax

```
set chassis slot <slot_list> console [no | yes]
```

Example

```
set chassis slot 6 console yes
```

enable chassis
contiguous_modem_
naming

This command enables the contiguous modem naming feature.

Syntax

```
enable chassis contiguous_modem_naming
```

Example

```
enable chassis contiguous_modem_naming
```

Related Commands

[disable chassis contiguous_modem_naming](#)

**disable chassis
contiguous_modem_
naming**

This command disables the contiguous modem naming feature.

Syntax

```
disable chassis contiguous_modem_ naming
```

Example

```
disable chassis contiguous_modem_ naming
```

Related Commands

[enable chassis contiguous_modem_ naming](#)

**Initialization Script
Commands****add init_script**

This command creates a modem initialization string, and adds it to the Init Script Table. Use [list init_scripts](#) to view current Init script Table entries. After you use the [set switched interface](#) command to assign an initialization script to a switched interface, that string will be sent to the serial line driver whenever a connection terminates, to ready the modem for the next connection. Generally speaking, you will not need to assign init scripts to modems. Maximum is 32 initialization scripts.



Do not use the default initialization script supplied with earlier firmware versions (NETServer releases 3.x). The `at&f1s0=1` script is invalid and may cause the router card's modem interfaces to lock up.

Syntax

```
add init_script <script name>
command <command string>
```

Table 90 Add Init_Script Command Parameters Descriptions

Parameter	Description	Settings
<script_name>	The designation of the init script.	Up to 7 ASCII characters.
command	Initialization string (AT commands). It must include double quotes. The CLI will append a /R and /N to it.	Up to 56 ASCII characters.

Related Commands

[delete init_script](#)

[list init_scripts](#)

[set init_script](#)

delete init_script This command removes a modem initialization string from the Init_script Table. Use [list init_scripts](#) to see which modem initialization scripts you have added.

Syntax

```
delete init_script <script_name>
```

Example

```
delete init_script test_script
```

Related Commands

[add init_script](#)

[list init_scripts](#)

[set init_script](#)

list init_scripts This command displays all the entries of Modem Initialization Table, which you previously defined using [add init_script](#). Initialization scripts are assigned to individual modems using the [set switched interface](#) command. The default initialization script USR_int carries the AT command ATSO=0. You can modify existing initialization scripts using the [set init_script](#) command.

Syntax

```
list init_script
```

Example

```
list init_script
```

Related Commands

[add init_script](#)

[delete init_script](#)

[set init_script](#)

set init_script This command modifies an init_script, that you previously defined using [add init_script](#). You can see the currently defined initialization scripts using [list init_scripts](#).



Do not use the default initialization script supplied with earlier firmware versions (NETServer 3.x). The at&f1s0=1 script is invalid and may cause the router card's modems to lock up.

Syntax

```
set init_script <script name>
command <string>
```

Table 91 Set INIT_Script Command Parameters Descriptions

Parameter	Description
<script name>	Designation for a modem initialization string. Maximum size is 7 characters. If you are setting an init_script for a modem pool or interface, the init_script name must already exist.
command	Modem initialization string must be entered with quotes, and be less than 56 characters.

Related Commands

[add init_script](#)
[delete init_script](#)
[list init_scripts](#)

Modem_group

enable modem_group This command enables the modem group you disabled with the [disable modem_group](#) command. Modem groups *all* and others incorporating installed modem cards (for example, *slot:3*) are provided as default modem groups, making system-wide or slot-by-slot enabling possible. Also see the [set modem_group](#) command, which configures all interfaces in the modem group.

Syntax

```
enable modem_group <name>
```

Example

```
enable modem_group mdmgrp15
```

Related Commands

[add modem_group](#)
[delete modem_group](#)
[disable modem_group](#)
[hangup modem_group](#)

[list_modem_groups](#)[set_modem_group](#)[show_modem_group](#)

hangup modem_group This command makes the modem group unavailable for dial-in users. This command has the same effect as hanging up the phone.

Syntax

```
hangup modem_group <name>
```

Example

```
hangup modem_group mdmgrp3
```

Related Commands[add_modem_group](#)[delete_modem_group](#)[disable_modem_group](#)[enable_modem_group](#)[list_modem_groups](#)[set_modem_group](#)[show_modem_group](#)

set modem_group This command configures a previously defined modem group. All the interfaces in the specified modem group are configured with this one command. Issue the [show interface <interface name> settings](#) command to view configuration.



Parameters set with this command are associated with the specified interface, not the modem group. Be aware that when you change parameters of interfaces assigned to multiple modem groups, the last change you make to a group containing any associated interface will reflect the latest configuration.



*When setting connection type, be aware that the `direct_net` parameter does **not** support the SLIP protocol. `Direct_net` requires the use of a negotiated protocol, which SLIP is not.*

Syntax

```
set modem_group <group_name>
    access [dial_in | dial_out | twoway]
    character_mode [even_seven_bit | no_parity_eight_bit |
    odd_seven_bit]
    connection_type [direct_conn | normal | direct_net | no_prompt
    | ppp_only | prompt_user_only]
    dial_prefix <string>
    disable_authentication [async_ppp | none | ppp | sync_ppp]
    dnis_authentication [disable | preferred | required]
    dnis_auth_time [before_answer | after_connect]
    dnis_auth_type [dnis | ani]
    dnis_password <ascii string>
    dnis_timeout <seconds>
    filter_access [on | off]
    host_address <IP_address or name>
    host_type [prompt | select | specified]
    init_script <name>
    input_filter <name>
    login_service [telnet | rlogin | cleartcp]
    login_table <string>
    message <login_message>
    output_filter <name>
    password <string>
    prompt <prompt_message>
    password_prompt <prompt_message>
    ppp_echo_request <0 to 5000>
    prompt_style [local | remote]
    prompt_delay <seconds>
    prompt_timeout <5, 600>
    protocol [ppp | slip]
    special_xon_xoff_flow [disabled | enabled]
    tcp_port <port_number>
    type [network | login | login_network]
    use_dnis_auth_pool [enabled | disabled | required ]
    user_name <user name>
```

Table 92 Set Modem_Group Command Parameters Descriptions

Parameter	Description
<group_name>	Designation of the modem group. Defaults: all, slot:1, slot:2, slot:3, etc. The limit is 64 ASCII characters.
access	Sets access type for switched interface. Modem can allow dial-in, dial-out or both (two-way). The default is two-way.
character_mode	Set the character mode for an interface. Options: even_seven_bit—Seven bit, even parity. no_parity_eight_bit—Eight bit, no parity. odd_seven_bit—seven bit odd parity. The default is no_parity_eight_bit.
connection_type	Sets the connection type for switched interface. Options: <ul style="list-style-type: none"> ■ Direct_net—Uses the protocol parameter's setting to create a network (virtual node) connection. Employs <i>user name</i> and <i>password</i> specified in this command. Authentication is done by the network protocol such as PPP. Direct_net <i>does not support</i> the SLIP protocol. ■ Direct_conn—Employs <i>user name</i> and <i>password</i> specified in this command to establish a login type connection to the target host. Authentication is accomplished by the target host. If user name and password are not specified with this choice, user "<i>default</i>" is employed. ■ Normal—Prompts for both <i>user name</i> and <i>password</i>. Default ■ Ppp_only—Configures a modem group for PPP only. After an incoming call is connected, PPP is started immediately. There is no prompting for login, and no default user authentication. If the peer does not respond to any of the LCP configuration request packets, the link is disconnected. Authentication is done using the negotiated PPP authentication. ■ Prompt_user_only—Prompts for <i>user name</i> only and authenticate with the <i>password</i> specified in this command. ■ No_prompt—Does not prompt. Authenticates with the <i>user name</i> and <i>password</i> specified in this command. If user name and password are not specified with this choice, user "<i>default</i>" is employed.
dial_prefix	Prefix added to all phone numbers dialing from this port. The limit is 64 ASCII characters.

Table 92 Set Modem_Group Command Parameters Descriptions (continued)

Parameter	Description
disable_authentication	<p>Sets enabling/disabling of authentication for types of dial-in users on a <i>per interface</i> basis. If authentication is disabled and a PPP call is auto-detected, the interface to which the user has dialed in will be checked for a configured user name which must previously have been entered using the <i>user_name</i> parameter in the above command. If <i>user_name</i> is specified for the particular interface, all user profile information will be forwarded without authentication. If no <i>user_name</i> is configured on the specified interface, <i>default</i> user's profile will be forwarded without authentication. The types of calls you can specify to disable authentication for are:</p> <ul style="list-style-type: none"> ■ None—Authentication is <i>not</i> disabled for any type of PPP call. Default ■ Async_ppp—Authentication is disabled if the incoming call is autodetected as a PPP <i>asynchronous</i> call ■ Sync_ppp—Authentication is disabled if the incoming call is autodetected as a PPP <i>synchronous</i> call. ■ PPP—Authentication is disabled if the incoming call is autodetected as a PPP call <p><i>Note:</i> When used, this feature disables all other types of authentication included local, RADIUS and TACACS+ authentication.</p>
dnis_authentication	<p>Specifies how to perform DNIS authentication. Options:</p> <p>disabled—No DNIS authentication is performed.</p> <p>preferred—If the incoming call has the required phone number information (ANI or DNIS), then DNIS authentication is attempted.</p> <p>required—If the incoming call does not have the required phone number information (ANI or DNIS), then the call is dropped. If the incoming call has the required phone number information (ANI or DNIS), DNIS authentication is attempted.</p>
dnis_auth_time	<p>Specifies when DNIS authentication is performed. Options:</p> <p>before_answer—Perform DNIS authentication before answering. Default</p> <p>after_connect—Perform DNIS authentication after connection is made.</p>
dnis_auth_type	<p>Specify which phone number will be used as user-name attribute. Options:</p> <p>dnis—Use the DNIS phone number.</p> <p>ani—Use the ANI phone number.</p>
dnis_password	<p>An ASCII string to be used as the user-password attribute. The limit is 64 ASCII characters.</p>
dnis_timeout	<p>Number of seconds to wait for DNIS authentication. The range is 0-60. A value of 0 disables this feature. The default value is 0.</p>
filter_access	<p>Turns filtering ON or OFF. The default is Off.</p>
host_address	<p>IP address to connect a dial-in user to, if the host type is specified, and connection type is <i>direct_conn</i> or <i>direct_net</i>.</p>
host_type	<p>Identifies how a dial in connection is set up. Options:</p> <ul style="list-style-type: none"> ■ prompt—prompted to enter host name or address. Default ■ select—a host is chosen from a login host list you specify, configured by the set connection command. ■ specified—connected to IP address configured here.

Table 92 Set Modem_Group Command Parameters Descriptions (continued)

Parameter	Description
input_filter	File name of filter screening incoming data.
init_script	Name of modem initialization script used. Maximum size: 7 ASCII characters. If you are setting an init_script for a Modem Pool or Interface the init_script name must already exist. A null string ("") indicates the name will be deleted. The default is USR_int.
login_service	The login service to use, if the connection type is not direct_net. Options: <ul style="list-style-type: none"> ■ TELNET—Default ■ RLOGIN ■ ClearTCP
message	The string to display to a dial-in user when a connection is set. The limit is 64 ASCII characters. Use the following values to display system information in the message line: <ul style="list-style-type: none"> ■ \$date—current date according to system uptime ■ \$callid—user's call identification according to system uptime ■ \$port—port occupied by user (slot:x/mod:y) ■ \$hostname—user's host name ■ \$sysname—user's system name (same as hostname) ■ \$time—time of call according to system uptime <p>Message information may also be defined in a banner file. To specify the banner file which contains the message text use the following command line syntax:</p> <p>Set modem_group <group_name> message <banner_file name></p> <p>If the message text includes spaces it <i>must</i> be enclosed in double quotations. Use the show user command to view the message as configured.</p> <p>See the set connection command for more information.</p>
output_file	File name of filter screening outgoing data.
password	Parameter used if the connection type is no_prompt or prompt_user_only. The limit is 63 ASCII characters.
prompt	String to present the dial-in user. The limit is 256 ASCII characters.
prompt_delay	The numbers of seconds to wait for a user to log in. Default is 0. Note: In most cases, you should use the default value of 0. If a value other than zero is used, and no successful user login has occurred within the specified time, the router card automatically logs the user in as the local user default using the default user's settings <i>without authentication</i> .
prompt_timeout	The maximum idle timeout for the username/password prompt for a dial-in connection. The default value is 5 minutes (300 seconds). If the prompt is idle for this time, the session will be terminated.
prompt_style	Specifies whether prompting of the username and password for the interface in this modem group will be provided by the router card (Local), or by a distant security service such as RADIUS or TACACS+ (remote). The default is Local.
protocol	Protocol to connect with, if the connection type is direct_net. SLIP is not supported by direct_net connection type. The default is PPP.

Table 92 Set Modem_Group Command Parameters Descriptions (continued)

Parameter	Description
special_xon_xoff_flow disabled	<p>Disables the special XON/XOFF flow control in the router card for terminal application for Dialup lines. When a XOFF character sent by a client reaches the router card, the router card should stop transmitting data to the modem. Once the router card receives XON, it should resume the data transfer.</p> <p>The default value is disabled. Only the terminal services (such as TELNET, CLEAR TCP dialin/dialout) will be affected by this configuration.</p> <p>For local users, use the following command to configure this feature: set user <name> special_xon_xoff_flow [disabled enabled]</p> <p>For RADIUS users, USR Vendor Specific Attribute 0x9879 configures this special flow control feature.</p> <p>Values 0 or Not Present - Disabled 1- Enabled</p>
special_xon_xoff_flow enabled	<p>Enables the special XON/XOFF flow control in the router card for terminal application for Dialup lines. See above item, special_xon_xoff_flow disabled.</p>
TCP_port	<p>TCP port number for the login host. Parameter used when connection type is <i>direct_conn</i> or <i>direct_net</i>. The limit is 65535.</p>
type	<p>Specifies type of connection allowed on interface.</p> <ul style="list-style-type: none"> ■ Login port only allows login users ■ Network port only allows network users ■ Login_network allows either type. Default
user_name	<p>Designation for the switched interface, used if connection type is no_prompt. The limit is 64 ASCII characters.</p>

Related Commands

[add_modem_group](#)

[delete_modem_group](#)

[disable_modem_group](#)

[enable_modem_group](#)

[hangup_modem_group](#)

[list_modem_groups](#)

[show_modem_group](#)

Network Management Card Commands

This section covers commands involving the network management card.

disable nmc chassis_awareness

This command disables the dynamic configuration of the chassis modems. If chassis configuration updates from the network management card are received, they are ignored. All chassis slot configuration must be done through the CLI, CFM load or SNMP sets.

Syntax

```
disable nmc chassis_awareness
```

Example

```
disable nmc chassis_awareness
```

Related Commands

[enable nmc chassis_awareness](#)

[enable nmc dynamic_slot_assignment](#)

[show nmc settings](#)

[show nmc status](#)

disable nmc dsa_idle_rebalancing

This command disallows idle modems to be periodically re-balanced by allowing slot ownership reassignment by the network management card. The default is disabled.

Syntax

```
disable nmc dsa_idle_rebalancing
```

Example

```
disable nmc dsa_idle_rebalancing
```

Related Commands

[enable nmc dsa_idle_rebalancing](#)

[show nmc settings](#)

[show nmc status](#)

**disable nmc
dynamic_slot_
assignment**

This command turns off the identification of chassis cards for dynamic slot assignment (DSA) in support of static load balancing and hot-standby fault tolerance.

Syntax

```
disable nmc dynamic_slot_assignment
```

Example

```
disable nmc dynamic_slot_assignment
```

Related Commands

[enable nmc chassis_awareness](#)

[enable nmc dynamic_slot_assignment](#)

[show nmc settings](#)

[show nmc status](#)

**disable nmc
snmp_forwarding**

This command turns off the snmp forwarding configuration of the chassis modems. The default is enabled.

Syntax

```
disable nmc snmp_forwarding
```

Example

```
disable nmc snmp_forwarding
```

**enable nmc
chassis_awareness**

This command enables the dynamic configuration of chassis modems. When chassis configuration updates from the network management card are received, they are used to update slot configuration. The default is enabled. Use the [show nmc settings](#) command to view edits.

Syntax

```
enable nmc chassis_awareness
```

Example

```
enable nmc chassis_awareness
```

Related Commands

[disable nmc chassis_awareness](#)

[enable nmc dynamic_slot_assignment](#)

[show nmc settings](#)

[show nmc status](#)

**enable nmc
dsa_idle_rebalancing**

This command allows idle modems to be periodically re-balanced by allowing slot ownership reassignment by the network management card. Slots are monitored for idleness and if idle slots are discovered to have caused unbalanced modem allocation, modems will be re-assigned to another slot. See [disable nmc dsa_idle_rebalancing](#) and commands for more information. The default is disabled.

Syntax

```
enable nmc dsa_idle_rebalancing
```

Example

```
enable nmc dsa_idle_rebalancing
```

Related Commands

[disable nmc dsa_idle_rebalancing](#)

**enable nmc
snmp_forwarding**

This command enables the snmp forwarding configuration of the chassis modems. The default is enabled.

Syntax

```
enable nmc snmp_forwarding
```

Example

```
enable nmc snmp_forwarding
```

**enable nmc
dynamic_slot_
assignment**

This command identifies cards in the Total Control Hub for dynamic slot assignment (DSA) to support static load balancing and hot-standby fault tolerance. The default is disabled.

DSA is an algorithm in the network management card which periodically polls chassis application cards for slots which support DSA. The network management card summarizes the information received and forwards that data to each router card, and on the basis of that data computes statically load-balanced slot assignments. New assignments are made every time a modem or application card is removed from or inserted in the Hub. DSA performs automatic load balancing whenever two or more application (router) cards are present in the chassis, assigning all calls, in turn, to successive router cards (Slot:1 - HiPer1, Slot:2 - HiPer2, Slot:3 - HiPer3, etc.). If a modem card reboots and is not statically assigned to a particular application card, then the modem slot is assigned to the application card with the least load.



*By default, when the router cards come up they are set to have ownership of all slots. It is very important that if you want to use DSA or have more than one router card, you properly configure slot ownership using the [set chassis slot](#) command. DSA will only reassign slots that have ownership of **no**.*

DSA is best suited for use as a “hot fail over” redundancy feature in the case where one router card fails and a second router card assumes ownership of all chassis cards. In this way, DSA can be employed in conjunction with static chassis card configuration to provide protection against a single point of failure. This type of configuration is advantageous when all chassis cards are supported by one router card with a second router card used as an emergency backup.

Syntax

```
enable nmc dynamic_slot_assignment
```

Example

In an example of a chassis containing 14 HDM cards and 2 router cards, CommWorks recommends that you do the following:

Enable chassis awareness with the **enable nmc chassis_awareness** command (**enabled** by default) and either:

- Enable DSA with the above command and set *slot ownership* of each slot to NO (**set chassis slot <x> owner no**)

or

- Statically configure each router card to own 7 modem cards each. The command used on each router card is **set chassis slot <x> owner yes**



In the case where a chassis slot is contested by the same router card, DSA will assign ownership of that slot to the router card occupying the lowest slot. Also, DSA never changes modem card ownerships unless a modem reboots or a router card reboots unless Idle Rebalancing is enabled. Then the system will periodically reassign modems to the router card when not in use.



When using fail-over make sure that you provide enough resources (IP addresses) on all the router cards to support this feature.

Related Commands

[enable nmc chassis_awareness](#)

[show nmc settings](#)

[show nmc status](#)

show nmc settings This command displays the current settings for the following network management card. See associated enable/disable commands for more information.

Syntax

```
show nmc settings
```

- **Chassis Awareness**—either **enabled** (default) or **disabled**
- **Dynamic Slot Assignment (DSA)**—either **enabled** or **disabled** (default)
- **DSA Idle Rebalancing**—either **enabled** or **disabled** (default)
- **SNMP Forwarding**—either **enabled** (default) or **disabled**.



DSA cannot be enabled unless chassis awareness is enabled. If chassis awareness is disabled, DSA is disabled as well. If DSA is enabled, chassis awareness is enabled as well. For example:

```
NMC SETTINGS
Chassis Awareness:      ENABLED
Dynamic Slot Assignment: ENABLED
DSA Idle Rebalancing:   ENABLED
SNMP Forwarding:       ENABLED
```

Example

```
show nmc settings
```

PBUS

list pbus sessions This command displays active pbus sessions based on interface name (one per modem connection) and includes the number of packets sent (*Spkts*) or received (*Rpkts*) and *packet size*. *Session* is the modem driver identifier.

Syntax

```
list pbus sessions
```

Example

```
list pbus sessions
```

Related Commands

[show pbus settings](#)

[list pbus traps](#)

list pbus traps This command displays the status of packet bus traps by interface as shown in the following example:

Syntax

```
list pbus traps
```

Example

```
list pbus traps
```

show pbus settings This command displays base setting and port density of modem slot/span/channel settings specified for packet bus modems. This affects vendor-specific fields in RADIUS authentication and accounting packets.

Syntax

```
show pbus settings
```

Example

```
show pbus settings
```

Related Commands

[set pbus reported_base](#)

[set pbus reported_port_density](#)

show sync interface This command displays the configuration of the specified V.35 interface. It lists the following information:

Syntax

```
show sync interface <physical_if_name>
```

- **NIC Type**—Type of network interface card
- **Speed**—Line speed
- **Flow Type**—Type of flow control used on this interface
- **Encoding**—Bit stream encoding type used for this interface
- **RTS Control**—Method used to control the Request to Send (RTS) signal
- **RTS-CTS Delay**—Interval (in milliseconds) that the DCE must wait after it sees RTS asserted before asserting CTS
- **Idle Pattern**—Bit pattern used to indicate an idle line
- **Minimum Flags**—Minimum number of flag patterns this port needs to recognize the end of one frame and the start of the next.
- **Clock Reference Mode**—Clock reference mode for this interface.

Clock Inverted Mode—Clock inverted mode for this interface. When set to **clockinverted** data is latched at the falling edge of the clock signal. When set to **none** data is latched at the rising edge of the clock signal.

Example

```
show sync interface <physical_if_name>
```

Datalink Frame Relay**set datalink
frame_relay interface**

This command sets the datalink frame relay interface

Syntax

```
set datalink frame_relay interface <interface_name>
    tracing [on |off]
    pvc_learning [on | off]
    polling_interval <5 to 30>
    mtu <260-2048>
    monitored_events <1 to 10>
    max_supported_pvc <number>
    management_type [no_lmi | lmi | itu |ansi]
    full_enquiry_interval <1 to 255>
    error_threshold <1 to 10>
    access_rate <0 to 8192000>
```

Related Commands

[show datalink frame_relay interface <interface_name> counters](#)

**show datalink
frame_relay interface
<interface_name>
counters**

This command displays statistics of the DLL created on top of the physical WAN interface.

Syntax

```
show datalink frame_relay interface <interface_name> counters
```

- **Transmitted Frames**—Sum of frames transmitted on this interface.
- **Transmitted Octets**—Sum of bytes transmitted on this interface.
- **Received Frames**—Sum of frames received on this interface.
- **Received Octets**—Sum of bytes received on this interface.
- **Unknown Errors**—Sum of errors whose cause is unexplained.
- **Received Short Frames**—Sum of errors caused by the reception of frames that were not long enough to allow de-multiplexing - the address field was incomplete, or for virtual circuits using Multiprotocol over Frame Relay, the protocol identifier was missing or incomplete.
- **Received Long Frames**—Sum of frames exceeding the maximum length configured for this interface.

- **Illegal DLCIs**—Sum of errors caused by the reception of LMI status frames containing illegal DLCIs.
- **Unknown DLCIs**—Sum of link maintenance frames containing an Information Element type invalid for the configured link maintenance protocol.
- **Protocol Errors**—Unspecified error occurred when attempting to interpret link maintenance frame.
- **Link Faults**—The number of times the interface has gone down since it was initialized.
- **Last Fault Time**—The system up time in days, minutes, hours and seconds at the time when the interface was taken down due to excessive errors. Excessive errors is defined as the time when a DLL exceeds the *Error Threshold* number within *Monitored Events* interval.

Related Commands

[set datalink frame_relay interface](#)

**show datalink
frame_relay interface
<interface_name> lmi
statistics**

This command displays Link Management Interface statistics of the DLL created on top of the physical WAN interface as specified by the *interface_name* parameter.

Syntax

```
show datalink frame_relay interface <interface_name> lmi
statistics
```

The following information is displayed:

LMI Protocol Statistics

- LMI Tx Frames—Sum of LMI packets transmitted by this DLL.
- LMI Rx Frames—Sum of LMI packets received by this DLL.
- LMI Tx Status Enquiry Frames—Sum of LMI Status Enquiry frames transmitted by this DLL.
- LMI Rx Status Enquiry Frames—Sum of LMI Status Enquiry frames received by this DLL.
- LMI Tx Status Frames—Sum of LMI Status frames transmitted by this DLL.
- LMI Rx Status Frames—Sum of LMI Status frames received by this DLL.
- LMI Rx Status Update Frames—Sum of LMI Status Update frames received by this DLL.
- No Response From Network Count—Number of LMI Status Enquiry frames that were unanswered by the network side.

LMI Protocol Error Counters

- Invalid Q.922 Header
- Invalid Control Field
- Invalid Protocol Discriminator Field
- Invalid Call Reference Field
- Invalid Message Type Field
- Invalid Locking Shift IE
- Invalid Report Type IE
- Invalid Link Integrity Verification IE
- Invalid Sequence Number
- Invalid PVC Status IE

LMI Received Unsolicited Message

- Unrecognized IE
- LMI Incomplete Message
- Out Of Order IE
- Invalid Spare Bits
- Invalid Extension Bit
- Invalid New, Active or Delete Bits

RS232

show rs232 interface This command displays the following settings for configured RS232 interfaces.

Syntax

```
show rs232 interface <interface_name_rsx>
    dte_in_sig
    dte_out_sig
    sync_errs
```

- **dte_in_sig**—Shows whether the data terminal equipment (DTE) CTS (clear to send) and DSR (data set ready) states are ON or OFF.
- **dte_out_sig**—Shows whether the DTE RTS (request to send) and DTR (data terminal ready) states are ON or OFF.
- **sync_errs**—Shows the quantity of following errors:
 - **Frame Checksum Errors**—Total number of frames with an invalid frame check sequence, input from the port since system re-initialization and while the port state was 'up' or 'test.'

- **Transmit Underrun Errors**—Total number of frames that failed to be transmitted on the port since system re-initialization and while the port state was 'up' or 'test' because data was not available to the transmitter in time.
- **Receive Overrun Errors**—Total number of frames that failed to be received on the port since system re-initialization and while the port state was 'up' or 'test' because the receiver did not accept the data in time.
- **Interrupted Frames**—Total number of frames that failed to be received or transmitted on the port due to loss of modem signals since system re-initialization and while the port state was 'up' or 'test.'
- **Aborted Frames**—Number of frames aborted on the port due to receiving an abort sequence since system re-initialization and while the port state was 'up' or 'test.'

TAP

add tap interface This command creates a data stream tap on the specified interface to log data to an off-line location. All data is captured in the stream, including protocol negotiation, then dumped to a SYSLOG host, the Console or a virtual (TELNET or dial-in) console port in *hexadecimal*, *ASCII*, or *clear* text. The router card permits multiple taps on different ports simultaneously.

When using the *SYSLOG* option, for each tap, data can be directed to one of eight priority locations, detailed above. Specifying facility and priority for each tap is useful if the remote SYSLOG daemons are set up to direct different facility and priority levels to different destination files or terminals.

When using the *screen* option, data from the tap is directed to the screen where the CLI command was issued. The CLI prompt will appear only when the tap is ended. A simple interface appears on screen with one option available. Press ESC and ENTER to stop a tap.

The configuration you choose to tap is not saved to FLASH memory so tap commands must be re-issued on system startup, but, a permanent user tap can be set using vendor-specific RADIUS attributes.



The monitor ppp command performs some similar functions as the tap command but is limited to PPP data streams only and provides PPP protocol decoding. Use tap commands to capture network traffic to a remote SYSLOG host or your console.

Issue the [delete tap](#) command to remove the tap from the table and [list tap](#) to view currently enabled taps.

Syntax

```

add tap interface <interface_name>

    address <IP_address>

    facility [log_auth | log_local0 | log_local1 | log_local2 |
log_local3 | log_local4 | log_local5 |
log_local6 | log_local7]

    format [hex | ascii | clear]

    loglevel [critical | unusual | common | verbose]

    output [screen | syslog]

```

Table 93 Add Tap Interface Command Parameters Descriptions

Parameter	Description
<interface_name>	The router card designation for the specific interface to be tapped. This is a modem interface specified as slot:x/mod:y.
address	Host name or IP address of the Unix host that will receive TAP information.
facility	The TAP node facility (site) where output is sent. See choices above. The default is log_auth.
format	The text style tap output is displayed as.
loglevel	Priority levels of messages that can be logged: <ul style="list-style-type: none"> ■ CRITICAL—a serious system error, which may effect system integrity. Default ■ UNUSUAL—an abnormal event, which the system should be able to recover from ■ COMMON—a regularly occurring event ■ VERBOSE—a regular periodic event, e.g. a routing update message
output	Endpoint where tap information can be directed: SCREEN or SYSLOG

Related Commands

[delete tap](#)

[list tap](#)

add tap next This command creates a tap on the next dial in or network connection. Tap output begins immediately upon next session startup. Press ESC and ENTER keys to exit tapping. Refer to the [add tap interface](#) command for more information. Issue the [delete tap](#) command to remove the tap from the table and [list tap](#) to view currently enabled taps.

Syntax

```
add tap next
    address <IP_address>
    facility [log_auth | log_local0 | log_local1 | log_local2 |
log_local3 | log_local4 | log_local5 |log_local6 | log_local7]
    format [hex | ascii | clear]
    loglevel [critical | unusual | common | verbose]
    output [screen | syslog]
```

Table 94 Add Tap Next Command Parameters Descriptions

Parameter	Description
address	Host name or IP address of the Unix host that will receive TAP information.
facility	The TAP node facility (site) where output is sent. See choices above. The default is log_auth.
format	The text style tap output is displayed as.
loglevel	Priority levels of messages that can be logged: <ul style="list-style-type: none"> ■ CRITICAL—a serious system error, which may effect system integrity. ■ UNUSUAL—an abnormal event, which the system should be able to recover from ■ COMMON—a regularly occurring event ■ VERBOSE—a regular periodic event, e.g. a routing update message. Default
output	Endpoint where tap information can be directed.

add tap user This command creates a tap on all currently active sessions of a specified user. Tap output begins immediately upon entering the command. Press ESC and ENTER keys to exit tapping. See the [add tap interface](#) command above for more information. Issue the [delete tap](#) command to remove the tap from the table and [list tap](#) to view currently enabled taps.

Syntax

```
add tap user <user_name>
      address <IP_address>
      facility [log_auth | log_local0 | log_local1 | log_local2 |
log_local3 | log_local4 | log_local5 |
log_local6 | log_local7]
      format [hex | ascii | clear]
      loglevel [critical | unusual | common | verbose]
      output [screen | syslog]
```

Table 95 Add Tap User Command Parameters

Parameters	Description
<user_name>	The router card designation for the specific user to be tapped. The limit is 64 ASCII characters.
address	IP address of the UNIX host that will receive TAP information.
facility	The TAP node facility (site) where output is sent. See choices above. The default is log_auth.
format	The text style tap output is displayed as.
output	Endpoint where tap information can be directed.
loglevel	Priority levels of messages that can be logged: <ul style="list-style-type: none"> ■ CRITICAL—a serious system error, which may effect system integrity. ■ UNUSUAL—an abnormal event, which the system should be able to recover from ■ COMMON—a regularly occurring event ■ VERBOSE—a regular periodic event, e.g. a routing update message. Default

delete tap This command removes the particular tap entry (1 to 99) or all entries you added to the tap table with the add tap command.

Syntax

```
delete tap [all | id 1 to 99]
```

Example

```
delete tap all
```

Related Commands

[add tap interface](#)

[add tap next](#)

[add tap user](#)

[list tap](#)

list tap This command displays all current tap settings specified with the [add tap interface](#), [add tap next](#), or [add tap user](#) commands.

Syntax

```
list tap
```

- **Id**—Tab entry in the table
- **Type**—Tap type. USER, SESSION, INT(ER)F(ACE)
- **Perm(anent)**—Whether tap is on continuously or not. Yes or No
- **Interface**—Modem where tap is being conducted
- **User**—Name of user whose output is being tapped
- **Out(put)**—Location where output is being directed. SCR(EE)N or SYSL(OG)
- **F(or)m(a)t**—Text style of output. HEX(ADECIMAL), ASC(II), or CL(EA)R
- **Facility**—Site where tap output is stored.
- **Lev(e)l**—Syslog level of tap output. CRIT(ICAL), UNUS(UAL), COMM(ON), VERB(OSE) - *Default*
- **Address**—SYSLOG host IP address

Example

```
list tap
```

Related Commands

[add tap interface](#)

[add tap next](#)

[add tap user](#)

set tap id This command configures a tap on a session previously created with the [add tap interface](#) command. Use the [delete tap](#) command to terminate the tap.

Syntax

```
set tap id <number>
    address <IP address>
    facility [log_auth | log_local0 | log_local1 | log_local2 |
log_local3 | log_local4 | log_local5 |log_local6 | log_local7]
    format [hex | ascii | clear]
    loglevel [critical | unusual | common | verbose]
```

Table 96 Set Tap ID Command Parameters

Parameters	Description
<number>	Identification number of particular tap to be configured which corresponds to tap entry in the table. The range is 1 to 99.
address	Syslog address where tap information is directed.
facility	Syslog facility where output is sent. See choices above. The default is log_auth.
format	Text style in which tap output is formatted. Choices: Hexadecimal, ASCII or clear text.
loglevel	Syslog loglevel to which output is assigned. See choices above.

Example

```
set tap id 5 address 10.10.3.3 facility log_auth format ascii
loglevel critical
```

delete tap id This command removes the specified tap on a session previously created.

Syntax

```
delete tap id <number>
```

Example

```
delete tap id 5
```

Related Commands

[list tap](#)

set tap user This command configures tap settings for the specified user as created by the [add tap user](#) command. Use the [delete tap](#) command to terminate the tap.

Syntax

```
set tap user <name>
    address <IP address>
    facility [log_auth | log_local0 | log_local1 | log_local2 |
log_local3 | log_local4 | log_local5 |log_local6 | log_local7]
    format [hex | ascii | clear]
    loglevel [critical | unusual | common | verbose]
    output <syslog>
    port_tap [disabled | enabled]
```

Table 97 Set Tap User Command Parameter

Parameters	Description
address	The syslog address where tap information is directed to.
facility	The syslog facility where output is sent. See choices above. The default is log_auth.
format	The text style in which the tap output is formatted. Choices: Hexadecimal, ASCII or Clear text.
loglevel	The syslog loglevel to which output is assigned. See choices above.
output	Tap output is directed to a syslog host.
port_tap	Switch to turn tap on or off for the specified user: Enabled or disabled.

Related Commands

[add tap user](#)

[delete tap](#)

6

ROUTING COMMANDS

This chapter describes the following routing commands:

- [Address Resolution Protocol Commands](#)
- [Asynchronous Transfer Mode](#)
- [DNS](#)
- [DNS](#)
- [Frame Relay](#)
- [ICMP](#)
- [L2TP](#)
- [PPTP](#)
- [MPIP](#)
- [Multicasting](#)
- [OSPF and Policy- Based Routing](#)
- [PPP](#)
- [PPPoE Commands](#)
- [Tunneling](#)

Address Resolution Protocol Commands

This section covers Address Resolution Protocol (ARP) commands of the CLI.

add atm_arp_server

This command creates a remote ATM ARP server for RFC-1577 compliant networks. The ATM ARP server (not a router card), which is queried to resolve IP mapping requests on the specified network, maps the IP addresses of connected servers to 20-byte ATM addresses.

Syntax

```
add atm_arp_server <name>
    atm_address <address>
    network <network name>
```

Table 98 Add ATM_ARP_Server Parameter Description

Parameter	Description
<name>	Designation of the ARP server to allow easy recognition and configuration on the router card. The limit is 32 ASCII characters.
atm_address	20-byte hexadecimal address of the NSAP (Network Service Access Point) ATM ARP server.
network	Designation of the network for which the ARP server is specified.

Example

```
add atm_arp_server arp_server atm_address
11.22.33.44.55.66.77.88.99.00.11.22.33.44.55.66.77.88.99.00
network ip_atm1577
```

For more configuration information, see the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Related Commands

[delete atm_arp_server](#)
[disable atm_arp_server](#)
[enable atm_arp_server](#)
[list atm_arp_server](#)
[show atm_arp_server](#)

**add ip arp address <IP
address>
access_mac_address
<MAC address>
interface <interface
name>**

This command adds static ARP entries and associates them with an interface. The IP and MAC address are required values. If an interface is not specified, the entry is applied to all interfaces.

Syntax

```
add ip arp address <IP address> access_mac_address <MAC address>
interface <interface name>
```

Table 99 Add IP ARP Address Command Parameters Descriptions

Parameter	Description	Settings
IP address	The IP address of the client that you are adding to the static ARP table.	xxx.xxx.xxx.xxx
MAC address	The MAC address of the client that you are adding to the static ARP table.	xx:xx:xx:xx:xx:xx
interface name	The interface that this client will be associated with in the static ARP table. If none is provided, the entry is applied to all interfaces.	Up to 32 ASCII characters

Related Commands

[add ip arp address <IP address> state \[private | public\]](#)

add ip arp address <IP address> state [private | public]

This command adds an IP address to the static ARP table and designates it as a public or private entry.

Syntax

```
add ip arp address <IP address> state [private | public]
```

Table 100 Add IP ARP Address Command Parameters

Parameter	Description
IP address	The IP address to add to the static ARP table.
state	private —Only check for a static ARP entry for the interface receiving the ARP request. public —If there isn't a static ARP entry for the current interface, check the table to see if the IP address is set for all interfaces.

Example

```
add ip arp address 10.10.3.3 state private
```

arp This command learns the IP address, and Media Access Control (MAC) address (Ethernet address) if on a locally connected network, of a network node via the Address Resolution Protocol (ARP). If the node is not in the ARP cache, an ARP request is sent out.

Syntax

```
arp <host name or IP address> output <output name file name>
```

Example

```
arp houston
```

The router card generates the following output

```
HiPer>> ARP: 156.155.132.145 -> 08:00:20:80:43:85
```

clear arp_cache

This command deletes all data in the ARP cache without rebooting the router card. Issue the [list ip arp](#) command to display ARP statistics.

Syntax

```
clear arp_cache
```

Example

```
clear arp_cache
```

delete atm_arp_server This command removes a remote ATM ARP server for RFC 1577-compliant networks which you added via the [add atm_arp_server](#) command. The configured entry must be disabled with the [disable atm_arp_server](#) command before it may be deleted.

Syntax

```
delete atm_arp_server <name>
```

Example

```
delete atm_arp_server chicago
```

Related Commands

[enable atm_arp_server](#)

[list atm_arp_server](#)

[show atm_arp_server](#)

delete ip arp address <IP address> interface <interface name> This command deletes the indicated IP address from the ARP table of the specified interface.

Syntax

```
delete ip arp address <IP address> interface <interface name>
```

Table 101 Delete IP ARP Address Command Parameters

Parameter	Description	Settings
IP address	The IP address to delete from the ARP table.	xxx.xxx.xxx.xxx
interface	The interface associated with the specified IP address.	Up to 32 ASCII characters.

Example

```
delete ip arp address 10.10.3.3 interface int1
```

disable atm_arp_server This command disconnects from and disables a remote ATM ARP server for RFC 1577-compliant networks that you added via the [add atm_arp_server](#) command. You must use this command to disable the configured entry before you can delete it using the [delete atm_arp_server](#) command.

Syntax

```
disable atm_arp_server <name>
```

Example

```
disable atm_arp_server chicago
```

Related Commands

[enable atm_arp_server](#)

[list atm_arp_server](#)

[enable authorization](#)

[show authorization](#)

[show atm_arp_server](#)

enable atm_arp_server This command re-enables a previously disabled remote ATM ARP server for RFC 1577-compliant networks which you added with the [add atm_arp_server](#) command.

Syntax

```
enable atm_arp_server <name>
```

Example

```
enable atm_arp_server chicago
```

Related Commands

[add atm_arp_server](#)

[delete atm_arp_server](#)

[disable atm_arp_server](#)

[list atm_arp_server](#)

[show atm_arp_server](#)

list ip arp This command displays the contents of the ARP cache.

Syntax

```
list ip arp
```

Table 102 List IP ARP Description

Parameter	Description
IP address	Network address for this entry.
Phys address	MAC address the IP address maps to.
Type	Ethernet interface type: Dynamic.
IfName	LAN interface name: eth:1 or eth:2.
State	Public or Private.

Example

```
list ip arp
```

show atm_arp_server This command displays settings for the particular ATM ARP server you configured with the [add atm_arp_server](#) command. The ATM ARP server maps IP addresses of connected servers to 20-byte ATM addresses. For more configuration information, refer to the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Syntax

```
show atm_arp_server <name>
```

Related Commands

[add atm_arp_server](#)

[delete atm_arp_server](#)

[disable atm_arp_server](#)

[enable atm_arp_server](#)

[list atm_arp_server](#)

Inverse Address Resolution Protocol Commands

This section covers commands that handle Inverse Address Resolution Protocol (ARP) configurations.

add ip invarp <IP address> type [dynamic | static]

This command adds static INVARP entries and associate them with an interface. The values <IP address> and <MAC addr> are required. If an interface is not specified, the entry is applied to all interfaces.

Syntax

```
add ip invarp <IP address> type [dynamic | static] pvc <string>
```

Example

```
add ip invarp 10.10.3.3 type dynamic pvc chicago
```

delete ip invarp

This command removes the specified static INVARP address.

Syntax

```
delete ip invarp <IP address>
```

Example

```
delete ip invarp 10.10.3.3
```

show ip invarp

This command displays inverse ARP information.

Syntax

```
show ip invarp
```

Table 103 Show IP INVARP Parameter Description

Parameter	Description
TX Interval	The transmission interval.
Max Age	The timeout age of an entry.
Network ID	The network ID of the ARP server.
Network Address	The network IP address corresponding to the physical address.
Physical Address	MAC address to which the IP address maps.
Type	The Ethernet interface type—either Dynamic, Invalid, Other, or Static.
Age	Timeout age of entry.

Example

```
show ip invarp
```

list ip invarp network This command displays the contents of the ARP cache.

Syntax

```
list ip invarp network <network name>
```

Table 104 List IP INVARP Network Description

Parameter	Description
IP address	Network address for this entry
Physical address	MAC address the IP address maps t
Type	Ethernet interface type: Dynamic
IfName	LAN interface name: eth:1 or eth:2

Example

```
list ip invarp network boston
```

invarp ptmp_pvc_group This command creates an inverse ARP point-to-multipoint permanent virtual connection group for PtMP calls. The group name can be up to 32 ASCII characters.

Syntax

```
invarp ptmp_pvc_group <net name>
```

Example

```
invarp ptmp_pvc_group chicago
```

Related Commands

[list ip invarp network](#)

invarp pvc This command creates an inverse ARP permanent virtual connection name, up to 32 ASCII characters.

Syntax

```
invarp pvc <net name>
```

Example

```
invarp pvc chicago
```

Related Commands

[list ip invarp network](#)

Asynchronous Transfer Mode

This section covers Asynchronous Transfer Mode (ATM) commands of the CLI.

add atm1483 pvc This command creates a Permanent Virtual Circuit (PVC) for RFC-1483 compliant networks. To configure multiple subnets, you must issue the command repeatedly, specifying different network names and addresses.

Syntax

```
add atm1483 pvc <name>
    address <IP address>
    interface <atmaal:1>
    network <network_name>
    peak <number>
    vci <number>
    vpi <number>
```

Table 105 Add ATM1483 PVC Command Parameters Descriptions

Parameter	Description	Settings
<name>	Designation for the PVC to allow easy recognition and configuration on the router card.	Up to 32 ASCII characters.
address	Network IP address for the far side of the PVC (router).	xxx.xxx.xxx.xxx
interface	This release supports only the <i>Span A</i> logical interface for independent configuration. The default is atmaal:1.	—
network	Designation of the network for which the PVC is specified.	—
peak	The peak bandwidth for this PVC in kilobits/second. The default is 0 (bandwidth = 1/10 of interface speed).	1000 to 10000
vci	Number of the Virtual Channel Indicator.	32 to 65535
vpi	Number of the Virtual Path Indicator. The default is 0.	0 to 255

Example

An example for combining IP and IPX:

```
add atm1483 pvc testing address 120.30.146.23 vci 200 vpi 1
network atm_network_1
```

```
add atm1483 pvc ip_over_atm address 204.220.145.43 vci 220 vpi 1 peak
100000 network ip_over_atm interface atmaal:1
```

Related Commands

[delete atm1483 pvc](#)
[disable atm1483 pvc](#)
[enable atm1483 pvc](#)
[list atm1483 pvcs](#)
[show atm1483 pvc <name>](#)

add atm1577 pvc This command Creates a Permanent Virtual Circuit (PVC) for classical IP and ARP support on RFC-1577 compliant networks. To configure multiple subnets, you must issue the command repeatedly, specifying different network names and addresses. For more configuration information, see the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*

Syntax

```
add atm1577 pvc <name>
    interface <atmaal:1>
    network <network name>
    peak <number>
    vci <number>
    vpi <number>
```

Table 106 Add ATM 1577 PVC Command Parameters Descriptions

Parameter	Description	Settings
<name>	Designation for the PVC to allow easy recognition and configuration on the router card. The limit is 32 ASCII characters.	Up to 32 ASCII characters
interface	This release supports only the <i>Span A</i> logical interface for independent configuration. The default is atmaal:1.	Any valid interface.
network	Designation of the network for which the PVC is specified.	Up to 32 ASCII characters.
peak	The peak bandwidth for this PVC in kilobits/second. The default is 0 (bandwidth = 1/10 of interface speed).	0 to 65535
vci	Number of the Virtual Channel Indicator.	32 to 65535
vpi	Number of the Virtual Path Indicator. The default is 0.	0 to 255

Related Commands

[delete atm1577 pvc](#)

[disable atm1577 pvc](#)

[enable atm1577 pvc](#)

[list atm1577 pvcs](#)

[show atm1577 pvc <name>](#)

delete atm1483 pvc This command removes a PVC you created for RFC-1483 compliant networks with the [add atm1483 pvc](#) command. For more configuration information, see *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Syntax

```
delete atm1483 pvc <name>
```

Related Commands

[add atm1483 pvc](#)

[disable atm1483 pvc](#)

[enable atm1483 pvc](#)

[list atm1483 pvcs](#)

[show atm1483 pvc <name>](#)

delete atm1577 pvc This command removes a PVC you created for RFC-1577 compliant networks with the [add atm1577 pvc](#) command. For more configuration information, see *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Syntax

```
delete atm1577 pvc <name>
```

Related Commands

[add atm1577 pvc](#)

[disable atm1577 pvc](#)

[enable atm1577 pvc](#)

[list atm1577 pvcs](#)

[show atm1577 pvc <name>](#)

disable atm1483 pvc This command disables a PVC you created for RFC-1483 compliant networks with the [add atm1483 pvc](#) command. For more configuration information, see *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Syntax

```
disable atm1483 pvc <name>
```

Related Commands

[add atm1483 pvc](#)

[delete atm1483 pvc](#)

[enable atm1483 pvc](#)

[list atm1483 pvcs](#)

[show atm1483 pvc <name>](#)

disable atm1577 pvc This command disables a PVC you created for RFC-1577 compliant networks with the [add atm1577 pvc](#) command. For more configuration information, see *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Syntax

```
disable atm1577 pvc <name>
```

Related Commands

[add atm1577 pvc](#)

[delete atm1577 pvc](#)

[enable atm1577 pvc](#)

[list atm1577 pvcs](#)

[show atm1577 pvc <name> settings](#)

disable atmsig This command disables the User-Network Interface (UNI) signaling configuration on the specified ATM network. For more configuration information, see *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Syntax

```
disable atmsig <name>
```

Example

```
disable atmsig chicago
```

Related Commands

[enable atmsig](#)

list atm1483 pvcs This command displays PVCS you created for RFC-1483 compliant networks with the [add atm1483 pvc](#) command. For more configuration information, see *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Syntax

```
list atm1483 pvcs
```

Example

```
list atm1483 pvcs
```

Related Commands

[add atm1483 pvc](#)

[delete atm1483 pvc](#)

[disable atm1483 pvc](#)

[enable atm1483 pvc](#)

[show atm1483 pvc <name>](#)

list atm1577 pvcs This command displays PVCs you created for RFC-1577 compliant networks with the [add atm1577 pvc](#) command. For more configuration information, see *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Syntax

```
list atm1577 pvcs
```

Example

```
list atm1577 pvcs
```

Related Commands

[add atm1577 pvc](#)

[delete atm1577 pvc](#)

[disable atm1577 pvc](#)

[enable atm1577 pvc](#)

[show atm1577 pvc <name> settings](#)

set atm options This command configures the ATM NIC's physical DS3 interfaces. For more configuration information, see *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Syntax

```
set atm options <interface name>
    cable_length [short_haul | long_haul]
    clock_source [network | internal]
    frame_type [adm | plcp]
    line_type [m23 | cbit | cchan | g832 | g751]
    payload_scrambling [on | off]
```

Table 107 Set ATM Options Command Parameters Descriptions

Parameter	Description
<interface name>	Designation of the physical DS3 interface name. Span A corresponds to ds3:1, Span B to ds3:2; e3:x, atmcell:x
cable_length	Allows the ATM NIC to be configured for long-haul (cable length between NIC and switch is between 0 and 450 feet) or short-haul (DSX-3, the cable length between the NIC and the switch is between 0 and 225 feet).
clock_source	Sets the timing source for the DS3 port. If the port is used as an independent port, the timing source should be configured for network (the source is the ATM switch). If the port is used to cascade additional NICs, the source should be configured for internal.
frame_type	Sets the method ATM cells are formatted: via ADM or the Physical Layer Convergence Protocol (PLCP). The default is ADM.
line_type	Sets the DS3 line implementing this circuit.
payload_scrambling	Minimizes the number of zero gaps in the packet stream, improving bandwidth efficiency.

set atm_address network This command configures an NSAP ATM address to establish an RFC-1577 SVC when the ATM switch being connected is a public switch or a private switch not supporting Interim Link Interface Management (ILMI) address registration. For more configuration information, see *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Syntax

```
set atm_address network <network name>
address <NSAP address>
```

Table 108 Set ATM_Address Network Command Parameters Descriptions

Parameter	Description
<network name>	Designation of the network for which the address is specified.
address	20-byte NSAP hexadecimal address (for the local network as configured on your switch) for use by SVCs on this network. E.g.: <i>ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff</i>

show atm1483 pvc <name> settings This command displays a specified PVC you created for RFC-1483 compliant networks with the [add atm1483 pvc](#) command. For more configuration information, see *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Syntax

```
show atm1483 pvc <name> settings
```

Related Commands

[add atm1483 pvc](#)

[delete atm1483 pvc](#)

[disable atm1483 pvc](#)

[enable atm1483 pvc](#)

[list atm1483 pvcs](#)

**show atm1577 pvc
<name> settings**

This command displays a specified PVC you created for RFC-1577 compliant networks with the [add atm1577 pvc](#) command. For more configuration information, see *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Syntax

```
show atm1577 pvc <name> settings
```

Related Commands

[delete atm1577 pvc](#)

[disable atm1577 pvc](#)

[enable atm1577 pvc](#)

[list atm1577 pvcs](#)

show atmcfg

This command displays the configuration for ATM interfaces (AAL) set with the [enable atmsig](#) and [enable ilmi](#) commands. For more configuration information, see the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Syntax

```
show atmcfg [atmaal:1 | atmaal:2]
```

Table 109 Show ATMCFG Parameter Descriptions

Parameter	Description
ATM Configuration	The specified ATM setting: Signaling and ILMI
Admin(istrative) Status	Whether the administrator has enabled or disabled the setting
Oper(ating) Status	Current state of the settingDial-Up LAN to LAN

Example

```
show atmcfg atmaal:1
```

**add ip defaultroute
gateway**

This command allows a default route to be configured. The command adds a default route with a gateway on the IP network configured on the first router card LAN interface (eth:1). This allows a default route to be configured.

A default route gateway specified with a lower metric acts as the *primary* default route gateway and a second default route gateway with a higher metric acts as the *secondary* default route gateway.

If one interface goes down, the default route gateway associated with that interface is disabled. If a second default route gateway associated with a still-alive interface exists, that gateway will be installed as the primary gateway.

If the disconnected interface is reconnected, the associated gateway will be re-installed.

Syntax

```
add ip defaultroute gateway <IP address or name>
    metric <hop count>
```

Table 110 Add IP Defaultroute Gateway Command Parameters Descriptions

Parameter	Description
<IP address>	IP address of the gateway router.
metric	An integer representing how far away the default router is, in hops through other routers. The range is 1-15. The default is 1.

Related Commands

[delete ip defaultroute gateway](#)
[set ip defaultroute gateway](#)

add ip network

This command adds an IP network to the list of IP networks available over the specified interface.



If you delete an IP network and it reappears following reboot, the reason may be that the Network Management Card was configured to automatically create an IP network for default route and minimal SNMP settings upon system startup.



Internal networks do not support SNAP encapsulation. Also, do not set the same internal IP address for more than one router card on the same LAN.

Syntax

```
add ip network <network name>
    address <IP network address>
    test frame [ethernet_ii|snap|atm1483|atm1577|fr1490|mcns]
    interface [eth:1|eth:2|internal|fr_pseudo_interface_name]
    enabled [yes | no]
    wan_type [unptp | nptp | network]
    remote_address <remote IP address and mask>
```

Table 111 Add IP Network Command Parameters Descriptions

Parameter	Description
network_name	Name of IP network, up to 32 ASCII characters. White space must be surrounded by double quotes.
address	IP address of the network, in the format nnn.nnn.nnn.nnn, with or without a mask specifier. The Mask Specifier can be 'A', 'B', 'C', or 'H', or a numeric value from 8 to 30 (32 for host) that describes the number of one bits in the mask. You can also specify the netmask in the xxx.xxx.xxx.xxx format. If you do not specify a mask, the system will generate it for you from the network address.
test frame	<p>Frame encapsulation to be used on this IP network.</p> <ul style="list-style-type: none"> ■ Ethernet_ii (default) ■ snap ■ atm1483 ■ atm1577 ■ fr1490 ■ mcns <p>Note: MCNS is not a valid choice even though it is listed.</p>
interface	Name of the interface which this IP network will communicate over. Eth:1 and Eth:2 are the two LAN ports available while internal is a setting to define a global or "interfaceless" IP address for the router card when supporting an on-demand or manual user with RIP over an <i>unnumbered</i> LAN-to-LAN connection. <i>fr_pseudo_interface_name</i> identifies the Frame Relay logical interface (PVC). The default is the first LAN interface (eth:1). See for more information.
enabled	Optional parameter indicates whether network is enabled (YES) or disabled (NO). Default is Yes.
wan_type	<p>For use in defining an IP network over a Frame Relay connection. Configures WAN connection as:</p> <ul style="list-style-type: none"> ■ UNPTP—Unnumbered Point-to-Point type of IP WAN connection. In this mode you must configure an IP address for the remote site only. You do not need to configure separate IP networks for the Frame Relay connection. The optional remote IP address should match the address defined in the remote router. If you are connecting to another router card over the Frame Relay connection, you do not need to provide a remote IP address. The IP address for the remote site will be learned via inverse Address Resolution Protocol (ARP). ■ NPTP—Numbered Point-to-Point type of IP WAN connection. In this mode you must configure an IP address for both the local and remote sites. ■ Network—Network type of IP WAN connection. In this mode you must configure an IP address for the local site only. This will emulate a broadcast network on the PVC.
remote_address	For Frame Relay only. Sets the IP address and IP mask for the remote end of the Frame Relay PVC. This parameter must be set if wan_type parameter is set up as NPTP.

Related Commands

[delete ip network](#)
[disable ip network](#)
[enable ip network](#)
[list ip networks](#)
[reconfigure ip network <network name>](#)
[set ip network <name>](#)
[show ip network <network_name> settings](#)

add ip route This command adds an IP static route entry to the IP Routing Table. IP packets destined for networks that match this network will be routed to this address. The [list ip routes](#) command displays all currently defined routes including the static route you create with this command but only if you have specified a *gateway*. Also see the [add ip defaultroute gateway](#) command.



Static routes are installed but not visible via the [list ip routes](#) command until the interface to the gateway is active (entered in the Forwarding Table).

Syntax

```
add ip route <IP address or host name>
      gateway <IP name or gateway address>
      metric <hop count>
```

Table 112 Add IP Route Command Parameters Descriptions

Parameter	Description
<IP address>	IP address or host name of the remote destination, in the format nnn.nnn.nnn.nnn, entered <i>with</i> or <i>without</i> a mask specifier. The mask specifier can be 'A', 'B', 'C', or 'H' (host), or a numeric value from 8 to 30 (32 if a host) that describes the number of one bits in the mask. You can also specify the netmask in the xxx.xxx.xxx.xxx format. If you do not specify a mask, the system will self-generate it (based on the network address) for all routes (<i>ip network address</i>) except <i>host</i> routes, for which you <i>must</i> specify a mask.
gateway	IP name or address of gateway used to reach this remote network.
metric	An integer for how distant the route is, in "hops", from the destination to the router card. The range is 1-15. The default is 1.

Related Commands

[delete ip route](#)
[disable ip static_remote_routes](#)
[enable ip static_remote_routes](#)
[set ip route <IP_hostname or network address>](#)

add framed_route user This command adds a framed (static) network to the user profile for dialup connections. This method of creating a static route does not run RIP to learn routes, so you must specify IP route and gateway addresses. For comparison, see the [add ip route](#) command.

Syntax

```
add framed_route user <name>
    gateway <IP address or name>
    ip_route <IP name or network address>
    metric <number>
```

Table 113 Add Framed_Route User Command Parameters Descriptions

Parameter	Description
<user name>	User name specified for the framed network, up to 32 ASCII characters.
gateway	IP address or name of the gateway used to reach this remote network.
ip_route	IP name or address of the remote network
metric	Integer representing how far away the route is, in "hops" from other routers. The default is 1. The range is 1-15.

Related Commands

[delete framed_route user](#)
[set framed_route user](#)

add ip source route <IP or net addr> gateway <IP name or addr> metric <metric> The router card supports routing based on source addresses of IP datagrams. When source based addressing is enabled, the IP packets coming in on a static interface are looked up in the routing table based on the source address instead of the destination address and routed accordingly. If source address lookup fails, the destination address is looked up and if that fails the default route is used.

Static routes must be added in the router card for the desired source addresses. The routes may be host routes or may be qualified with a net-mask. These routes are not propagated via RIP or OSPF. The feature can be turned on for a static interface (Ethernet, leased line etc.) and all incoming IP datagrams are routed based on source addresses.

Syntax

```
add ip source route <IP or net addr> gateway <IP name or addr>
metric <metric>
```

Table 114 Add IP Source Route Command Parameters Descriptions

Parameter	Description
source route	The network name or IP address of the source of the IP datagram.
gateway	The network name or IP address of the gateway to which IP datagrams with the specified source address should be routed.
metric	This specifies how many hops it is to the specified gateway.

add ipx network This command adds an IPX network to the list of IPX networks available over the specified interface.

Syntax

```

add ipx network <network name>
    address <IPX network address>
    interface [eth:1 | eth:2 | fr_pseudo_interface_name]
    enabled [yes | no]
    frame [ethernet_ii | snap | dsap | novell_8023 | fr1490]

```

Table 115 Add IPX Network Command Parameters Descriptions

Parameter	Description
<network_name>	Name of IPX network. Unique ASCII string of up to 32 characters.
address	Address of the IPX network.
interface	Name of interface with which this IPX network will associate. For Frame Relay, <i>fr_pseudo_interface_name</i> identifies the Frame Relay logical interface (PVC). The default is the first LAN interface (eth:1).
enabled	Optional parameter indicates whether network is enabled (YES) or disabled (NO). The default is YES.
frame	Frame encapsulation to be used on this IPX network. Choices: <ul style="list-style-type: none"> ■ Ethernet_II—default Ethernet frame type. Default ■ SNAP (Ethernet_SNAP)—Sub-Network Access Protocol derived from 802.2 ■ DSAP (802.2)—default frame type for NetWare v4.x ■ Novell_8023 (802.3 raw)—default frame type for NetWare v2.x and v3.x networks ■ fr1490—default frame type for Frame Relay networks.

Related Commands

[delete ipx network](#)

[disable ipx network](#)

[enable ipx network](#)

[list ipx networks](#)

[set ipx network](#)

[show ipx network <network name> settings](#)

[show ipx network <network_name> counters](#)

add ipx route This command adds an IPX static route to the system's IPX Route Table, which defines static routes to remote IPX networks. The command `list ipx routes` displays currently defined static routes.

Syntax

```
add ipx route <IPX network address>
    gateway <IPX host address>
    metric [1 to 15]
    ticks <tick number>
```

Table 116 Add IPX Route Command Parameters Descriptions

Parameter	Description
<ipx_net_address>	IPX network address requiring a route.
gateway	IPX address of the host which will act as a gateway. The format is nnnn.xx:xx:xx:xx:xx:xx (network_address.mac_address).
metric	Number of hops through different routers to reach the remote IPX network. The range is 1-15.
ticks	Estimated interval in ticks it takes to deliver a packet to the remote network. There are approximately 18 ticks per second.

Related Commands

[delete ipx route](#)

[list ipx routes](#)

add ipx service This command adds a static IPX service to the IPX Services Table. You must supply the name, internal IPX network number, node number, socket, and type of service for this service. You must also supply gateway information to indicate the next router hop.

Syntax

```
add ipx service <service_name>
    address <internal network address>
    gateway <network_number.mac_address>
    metric [1 to 15]
    node <internal node number>
    socket <socket number>
    type <service type>
```

Table 117 Add IPX Service Command Parameters Descriptions

Parameter	Description
<service name>	Designation of IPX service. The limit is 32 ASCII characters.
address	Internal network number for the IPX service on which this service resides.
gateway	Host address of the router you defined as the gateway.
metric	Integer representing how far away the default router is, in hops through other routers. The range is 1-15.
node	The internal node number (MAC address) of the server on which the service resides. Typically 00:00:00:00:00:01.
socket	The port the server listens on. Socket numbers are the joined sender's (or receiver's) IPX address and service type's port number.
type	Type of service. Hexadecimal number referring to file server, print server, etc. Refer to the table below.

[Table 118](#) lists the codes for the types of IPX services.

Table 118 IPX Service Types and Descriptions

IPX Service Type	Description	IPX Service Type	Description
04	file server	7A	TES-NetWare VMS
05	job server	98	NetWare access server
07	print server	9A	Named Pipes server
09	archive server	9E	PortableNetWare-UNIX
0A	job queue	107	NetWare 386
21	NAS SNA gateway	111	Test server
2E	dynamic SAP	166	NetWare management
47	advertising print server	26A	NetWare management
4B	Btrieve VAP 5.0	26B	Time synchronization
4C	SQL VAP	278	NetWare Directory server
IPX Service Type	Description	IPX Service Type	Description
04	file server	7A	TES-NetWare VMS
05	job server	98	NetWare access server
07	print server	9A	Named Pipes server
09	archive server	9E	PortableNetWare-UNIX
0A	job queue	107	NetWare 386
21	NAS SNA gateway	111	Test server
2E	dynamic SAP	166	NetWare management
47	advertising print server	26A	NetWare management
4B	Btrieve VAP 5.0	26B	Time synchronization
4C	SQL VAP	278	NetWare Directory server

Related Commands

[delete ipx service](#)

[delete ipx service_all](#)

[list ipx services](#)

delete ip defaultroute gateway This command deletes the IP default route created with the [add ip defaultroute gateway](#) command. Use the [list ip routes](#) command to verify edit.

Syntax

```
delete ip defaultroute gateway <IP_address or name>
```

Example

```
delete ip defaultroute gateway 10.10.3.3
```

Related Commands

[add ip defaultroute gateway](#)

[set ip defaultroute gateway](#)

delete ip network This command deletes an IP network from the interface that you specified when *adding* the network. Use [list ip networks](#) to see which networks are associated with which interfaces. Always use [disable ip network](#) before deleting it.

Syntax

```
delete ip network <network_name>
```

Example

```
delete ip network boston2
```

Related Commands

[add ip network](#)

[disable ip network](#)

[enable ip network](#)

[list ip networks](#)

[reconfigure ip network <network name>](#)

[set ip network <name>](#)

[show ip network <network_name> settings](#)

delete ip pool This command deletes an IP pool created with the [add ip pool](#) command. Use the [list ip pools](#) command to verify edit.



This command takes effect only after all addresses have been released from the pool. Also, when a IP pool is deleted, be sure to also delete the pool from any associated user's profile.

Syntax

```
delete ip pool <pool name>
```

Example

```
delete ip pool boston
```

Related Commands

[add address_pool user](#)

[add ip pool](#)

[delete address_pool user](#)

[enable ip address_pool_filtering](#)

[list ip pools](#)

[set ip pool](#)

delete ip route This command deletes the *specified* static/learned IP address or *all* learned routes (including RIPv1/RIPv2 routes) from the IP Routing Table. The *subnet mask* value, which is optional, takes the form of *A, B, C* and *H*, or a numeric value from *8 to 32*. It also accepts dot format, in which case the value must be *255.0.0.0* or *greater* and *contiguous*. Deleting routes will cause IP packets destined for those networks to use the default route which can be viewed using the [list ip routes](#) command. Refer to the [add ip defaultroute gateway](#) and [add ip route](#) commands for more information.

Syntax

```
delete ip route <network name or IP address/subnet_mask>
    all_learned_routes
```

Related Commands

[add ip route](#)

[list ip routes](#)

[set ip route <IP_hostname or network address>](#)

delete ip source route This command deletes the specified source route from the routing table. Specify the source route by its network name or IP address.

Syntax

```
delete ip source route <IP name or net address>
```

Example

```
delete ip source route 10.10.3.3
```

delete ipx network This command deletes an IPX network on the interface you specified with the [add ipx network](#) command. You can use [list ipx networks](#) to see which are available, and the network's status. Use the [disable ipx network](#) command before deleting the network.

Syntax

```
delete ipx network <network name>
```

Example

```
delete ipx network chicago
```

Related Commands

[add ipx network](#)

[disable ipx network](#)

[enable ipx network](#)

[list ipx networks](#)

[set ipx network](#)

[show ipx network <network name> settings](#)

[show ipx network <network_name> counters](#)

delete ipx route This command deletes a specified route or *all* IPX and learned (RIPv1/v2) routes on the interface you created with the [add ipx route](#) command. The [list ipx routes](#) command displays the current IPX routes.

Syntax

```
delete ipx route <IPX network address> all
```

Related Commands

[add ipx route](#)

[list ipx routes](#)

delete ipx service This command deletes static or learned IPX routes configured with the [add ipx service](#) command. This command works only if a complete match on all parameters is found.

Syntax

```
delete ipx service <service_name>
      type <service_type>
```

Table 119 Delete IPX Service Command Parameters Descriptions

Parameter	Description
<service name>	Designation of IPX service. The limit is 32 ASCII characters.
type	Type of service, file/server, print, etc., expressed in hexadecimal format (xxxxxx).

Related Commands

[add ipx service](#)
[delete ipx service_all](#)
[list ipx services](#)

delete ipx service_all This command deletes all IPX *learned* routes from the IPX Static Services Table.

Syntax

```
delete ipx service_all
```

Example

```
delete ipx service_all
```

Related Commands

[add ipx service](#)
[delete ipx service](#)
[list ipx services](#)

disable ip This command disables IP broadcast parameters.

Syntax

```
disable ip
      directed_bcast_forwarding
      multicast_affect_inactivity
      respond_to_directed_bcast
      send_host_unreach_for_pool
```

Table 120 Disable IP Command Parameters Descriptions

Parameter	Description
directed_bcast_forwarding	If there is a directed broadcast packet coming for the router card's directly connected network, the router card will forward that packet to the interface depending on this configuration. Directed broadcast will be forwarded only if the Destination IP address of the packet matches with the broadcast route installed for the interface. Default is disabled.
multicast_affect_inactivity	When this is disabled the IGMP download traffic does not affect PPP inactivity timer. In effect if the user keeps some multicast operation on but does not download anything else, he/she will be disconnected after configured inactivity timeout. When it is enabled, multicast traffic is treated as any other traffic. And inactivity timeout does not occur. Note that count /not count multicast packets passing through a connection are an <i>activity</i> . If inactivity timeout is configured for that connection, then if there is no activity for the configured time period the connection will be disconnected.
respond_to_directed_bcast	Disables the router card from responding to the ICMP requests, or generating ICMP error messages for packets coming to a directed broadcast address of its networks.
send_host_unreach_for_pool	When disabled, if the address is a part of the configured IP Address Pool, the router card does not send the ICMP host an unreachable message (irrespective of any routing information).

disable ip address_pool_filtering

This command disables packet filtering on all IP address pools (drops packets for IP addresses within IP pools not in use). For more information, refer to the Total Control 1000 Enhanced Data System Documentation Library.

Syntax

```
disable ip address_pool_filtering
```

Example

```
disable ip address_pool_filtering
```

Related Commands

[add address_pool user](#)

[add ip pool](#)

[delete address_pool user](#)

[enable ip address_pool_filtering](#)

[set ip pool](#)

**disable ip
address_pool_
round_robin**

This command turns off round robin allocation of IP addresses from IP address pools configured with the [add ip pool](#) command. The default is enabled.

Syntax

```
disable ip address_pool_round_robin
```

Example

```
disable ip address_pool_round_robin
```

Related Commands

[add ip pool](#)

[enable ip address_pool_round_robin](#)

[show ip settings](#)

disable ip forwarding

This command causes the system to stop forwarding any packets over IP networks but the router card will still operate as a client. Under most circumstance, you would never disable forwarding. You may want to disable IP forwarding if you are using the system only as a terminal server since users who telnet to the system can still connect to remote hosts.

Syntax

```
disable ip forwarding
```

Example

```
disable ip forwarding
```

Related Commands

[enable ip forwarding](#)

[show ip settings](#)

**disable ip ia_force_
nexthop_route**

When disabled, and the configured IEA next hop routing interface is unreachable, the router card can still direct user traffic using other routing information, including the default gateway. The default is disabled.

Syntax

```
disable ip ia_force_nexthop_route
```

Example

```
disable ip ia_force_nexthop_route
```

Related Commands

[enable ip ia_force_nexthop_route](#)

[show ip network <network_name> settings](#)

**disable ip
iea_next_hop_routing**

This global configuration disables IEA next hop routing when packets are received from the dial-in user. When disabled, packets from the user are sent to a destination host on the local network or the configured default gateway. Use the [show ip network <network_name> settings](#) command to view the current IEA next hop gateway. The default is enabled.

Syntax

```
disable ip iea_next_hop_routing
```

Example

```
disable ip iea_next_hop_routing
```

Related Commands

[enable ip iea_next_hop_routing](#)

[show ip network <network_name> settings](#)

**disable ip
multicast_heartbeat**

This command disables multicast monitoring for a specified multicast group or interface.

Syntax

```
disable ip multicast_heartbeat
```

Example

```
disable ip multicast_heartbeat
```

Related Commands

[enable ip multicast_heartbeat](#)

[set ip multicast_heartbeat](#)

[show ip settings](#)

disable ip network This command disables the specified IP network. Make sure there is no activity on this network before disabling it.

Syntax

```
disable ip network <network_name>
```

Example

```
disable ip network boston1
```

Related Commands

[add ip network](#)

[delete ip network](#)

[enable ip network](#)

[list ip networks](#)

[reconfigure ip network <network name>](#)

[set ip network <name>](#)

[show ip network <network_name> settings](#)

disable ip proxy_arp_all_dialin This command disables the sending of a proxy ARP response for dial-in IP addresses even if they are not part of the LAN. This feature is disabled by default.

Syntax

```
disable ip proxy_arp_all_dialin
```

Example

```
disable ip proxy_arp_all_dialin
```

Related Commands

[enable ip proxy_arp_all_dialin](#)

disable ip rip This command disables the RIP routing algorithm on all IP networks. Use [show ip routing settings](#) to see the current status of IP routing. This saves system space by preventing a large RIP database, which is useful for networks connecting over the WAN interface.

Syntax

```
disable ip rip
```

Example

```
disable ip rip
```

Related Commands

[enable ip rip](#)
[set ip network <name>](#)
[disable ip routing](#)
[enable ip routing](#)
[show ip routing settings](#)

disable ip routing This command disables all routing protocols on all IP networks. Currently, the only routing protocol is RIP, which means that [disable ip rip](#) performs the same function. Use the [show ip routing settings](#) command to see the current status of IP routing.

Syntax

```
disable ip routing
```

Example

```
disable ip routing
```

Related Commands

[show ip routing settings](#)
[disable ip rip](#)

disable ip send_unsolicited_arp This command disables the sending of unsolicited ARP messages once the dial-in user is connected. Use the [enable ip send_unsolicited_arp](#) command to turn this feature on. The default is disabled.

Syntax

```
disable ip send_unsolicited_arp
```

Example

```
disable ip send_unsolicited_arp
```

Related Commands

[enable ip send_unsolicited_arp](#)

disable ip send_host_unreach_for_pool This command disables the sending of unreachable hosts from the pool.

Syntax

```
disable ip send_host_unreach_for_pool
```

Example

```
disable ip send_host_unreach_for_pool
```

**disable ip
source_address_filter**

This command disables filtering of packets that bear a source IP address other than that assigned by the router card during negotiations. This should not be enabled for LAN-to-LAN routing. This feature is disabled by default.

Syntax

```
disable ip source_address_filter
```

Example

```
disable ip source_address_filter
```

Related Commands

[enable ip source_address_filter](#)

**disable ip
static_remote_routes**

This command disables all statically defined remote routes on all IP networks, [add ip route](#) command. You can list the current IP routes using the [list ip routes](#) command.

Syntax

```
disable ip static_remote_routes
```

Example

```
disable ip static_remote_routes
```

Related Commands

[add ip route](#)

[delete ip route](#)

[disable ip static_remote_routes](#)

[enable ip static_remote_routes](#)

[list ip routes](#)

disable ipx network

This command disables the specified IPX network. Use [list ipx networks](#) to see which IPX networks are defined, and their current status.

Syntax

```
disable ipx network <network_name>
```

Example

```
disable ipx network <network_name>
```

Related Commands

[add ipx network](#)
[delete ipx network](#)
[enable ipx network](#)
[list ipx networks](#)
[set ipx network](#)
[show ipx network <network name> settings](#)
[show ipx network <network_name> counters](#)

disable ipx rip network This command disables the RIP routing protocol on the specified IPX network. This saves system space by barring a large RIP database from growing, which is useful for networks connecting over the WAN interface. Use the [enable ipx rip network](#) command to restart RIP on this IPX network.

Syntax

```
disable ipx rip network <network name>
```

Example

```
disable ipx rip network chicago
```

Related Commands

[show ipx](#)
[show ipx rip settings](#)

disable ipx sap network This command disables the Service Advertising Protocol (SAP) on the specified network. This saves system space by barring a large SAP database from growing, which is useful for networks connecting over the WAN interface. Use the [enable ipx sap network](#) command to restart SAP on this IPX network.

Syntax

```
disable ipx sap network <network_name>
```

Example

```
disable ipx sap network chicago
```

Related Commands

[enable ipx sap network](#)
[show ipx network <network name> settings](#)
[show ipx sap](#)
[show ipx sap settings](#)

enable ip This command enables IP broadcast parameters.

Syntax

```
enable ip
    directed_bcast_forwarding
    multicast_affect_inactivity
    respond_to_directed_bcast
    send_host_unreach_for_pool
```

Table 121 Enable IP Command Parameters Descriptions

Parameter	Description
directed_bcast_forwarding	If there is a directed broadcast packet coming for the router card's directly connected network, the router card will forward that packet to the interface depending on this configuration. Directed broadcast will be forwarded only if the Destination IP address of the packet matches with the broadcast route installed for the interface. Default is disabled.
multicast_affect_inactivity	When this is disabled the IGMP download traffic does not affect PPP inactivity timer. In effect if the user keeps some multicast operation on but does not download anything else, he/she will be disconnected after configured inactivity timeout. When it is enabled, multicast traffic is treated as any other traffic. And inactivity timeout does not occur. Note that count /not count multicast packets passing through a connection are an <i>activity</i> . If inactivity timeout is configured for that connection, then if there is no activity for the configured time period the connection will be disconnected.
respond_to_directed_bcast	Disables the router card from responding to the ICMP requests, or generating ICMP error messages for packets coming to a directed broadcast address of its networks.
send_host_unreach_for_pool	When disabled, if the address is a part of the configured IP Address Pool, the router card does not send the ICMP host an unreachable message (irrespective of any routing information).

Related Commands

[enable ip address_pool_filtering](#)
[enable ip address_pool_round_robin](#)
[enable ip forwarding](#)
[enable ip iea_force_nexthop_route](#)
[enable ip iea_next_hop_routing](#)
[enable ip multicast_heartbeat](#)
[enable ip network](#)

enable ip address_pool_filtering This command permits packet filtering on all IP address pools. Use the [show ip settings](#) command to view the current setting.

Syntax

```
enable ip address_pool_filtering
```

Example

```
enable ip address_pool_filtering
```

Related Commands

[add address_pool user](#)

[add ip pool](#)

[delete address_pool user](#)

[disable ip address_pool_filtering](#)

[show ip settings](#)

[set ip pool](#)

enable ip address_pool_round_robin This command turns on round robin allocation of IP addresses from IP address pools configured with the [add ip pool](#) command. Use the [show ip settings](#) command to view the current setting. The default is enabled.

Syntax

```
enable ip address_pool_round_robin
```

Example

```
enable ip address_pool_round_robin
```

Related Commands

[add ip pool](#)

[disable ip address_pool_round_robin](#)

[show ip settings](#)

enable ip forwarding This command allows all IP networks to forward (route) packets.

Syntax

```
enable ip forwarding
```

Example

```
enable ip forwarding
```

Related Commands

[disable ip forwarding](#)

[show ip settings](#)

**enable ip ia_force_
nexthop_route**

This command forces the system to disconnect the dial-in user if the configured IEA next hop routing interface is unreachable. When disabled, and the configured next hop routing interface is unreachable, the router card can still direct user traffic using other routing information, including the default gateway. Use the [show ip network settings](#) command to view the current IEA next hop gateway. The default is disabled.

Syntax

```
enable ip ia_force_nexthop_route
```

Example

```
enable ip ia_force_nexthop_route
```

Related Commands

[disable ip ia_force_nexthop_route](#)

[show ip network settings](#)

**enable ip
ia_next_hop_routing**

This global configuration indicates whether to apply IEA next hop routing when packets are received from dial-in user. Use the [show ip network settings](#) command to view the current IEA next hop gateway. The default is enabled.

Syntax

```
enable ip ia_next_hop_routing
```

Example

```
enable ip ia_next_hop_routing
```

Related Commands

[disable ip ia_next_hop_routing](#)

[show ip network settings](#)

**enable ip
multicast_heartbeat**

This command enables multicast monitoring for a specified multicast group or interface.

Syntax

```
enable ip multicast_heartbeat
```

Example

```
enable ip multicast_heartbeat
```

Related Commands

[disable ip multicast_heartbeat](#)

[set ip multicast heartbeat](#)

[show ip settings](#)

enable ip network This command enables the specified IP network, which you previously defined using [add ip network](#). You can use [list ip networks](#) to see the currently defined IP networks, as well as their current status.

Syntax

```
enable ip network <network_name>
```

Example

```
enable ip network chicago
```

Related Commands

[add ip network](#)

[delete ip network](#)

[disable ip network](#)

[list ip networks](#)

[reconfigure ip network <network name>](#)

[set ip network <name>](#)

[show ip network <network_name> settings](#)

enable ip proxy_arp_all_dialin This command enables the sending of a proxy ARP response for dial-in IP addresses even if they are not part of the LAN. This feature is disabled by default.

Syntax

```
enable ip proxy_arp_all_dialin
```

Example

```
enable ip proxy_arp_all_dialin
```

Related Commands

[disable ip proxy_arp_all_dialin](#)

enable ip rip This command enables the RIP protocol for all IP networks. RIP protocol is set to NONE by default.

Syntax

```
enable ip rip
```

Example

```
enable ip rip
```

Related Commands

[disable ip rip](#)

[disable ip routing](#)

[enable ip rip](#)

[show ip routing settings](#)

enable ip routing This command allows all routing protocols for all IP networks. Currently, this command enables only RIP, so it is functionally the same as enable ip rip. Use the [show ip routing settings](#) command to view the current setting.

Syntax

```
enable ip routing
```

Example

```
enable ip routing
```

Related Commands

[disable ip routing](#)

[enable ip rip](#)

[enable ip routing](#)

[show ip routing settings](#)

enable ip send_unsolicited_arp This command indicates whether to send unsolicited ARP messages once the dial-in user is connected. Use the [disable ip send_unsolicited_arp](#) command to turn this feature off. The default is disabled.

Syntax

```
enable ip send_unsolicited_arp
```

Example

```
enable ip send_unsolicited_arp
```

Related Commands

[disable ip send_unsolicited_arp](#)

**enable ip
source_address_filter**

This command enables filtering of packets that bear a source IP address other than that assigned by the router card during negotiations. This should not be enabled for LAN-to-LAN routing. This feature works for both PPP and SLIP users. This feature is disabled by default.

Syntax

```
enable ip source_address_filter
```

Example

```
enable ip source_address_filter
```

Related Commands

[disable ip source_address_filter](#)

**enable ip
static_remote_routes**

This command enables statically defined remote routes, which are defined with the [add ip route](#) command.

Syntax

```
enable ip static_remote_routes
```

Example

```
enable ip static_remote_routes
```

Related Commands

[add ip route](#)

[delete ip route](#)

[disable ip static_remote_routes](#)

[enable ip static_remote_routes](#)

[list ip routes](#)

enable ipx network This command enables the specified IPX network. Use [add ipx network](#) to define IPX networks.

Syntax

```
enable ipx network <network name>
```

Example

```
enable ipx network chicago
```

Related Commands

[add ipx network](#)

[delete ipx network](#)

[disable ipx network](#)

[list ipx networks](#)

[set ipx network](#)

[show ipx network <network name> settings](#)

[show ipx network <network name> counters](#)

enable ipx rip network This command enables the RIP protocol for the specified IPX network. RIP is normally enabled when you add an IPX network. You can see if RIP is currently enabled (ON) using the [show ipx rip settings](#), [show ipx network <network name> settings](#), or [show ip network settings](#) commands.

Syntax

```
enable ipx rip network <network_name>
```

Example

```
enable ipx rip network boston
```

Related Commands

[disable ipx rip network](#)

[show ipx rip settings](#)

enable ipx sap network This command enables the Service Advertising Protocol (SAP) on the specified network. SAP is normally enabled when you add an IPX network. Use [show ipx sap settings](#) or [show ipx network <network name> settings](#) to determine the current state of the IPX SAP network.

Syntax

```
enable ipx sap network <network_name>
```

Example

```
enable ipx sap network chicago
```

Related Commands

[disable ipx sap network](#)
[show ipx network <network name> settings](#)
[show ipx sap settings](#)
[show ipx sap settings](#)

list ip networks This command displays all the IP networks you previously defined *statically* using the add ip network command and any dynamic networks created with a modem-established PPP/SLIP connection to the router card. It also lists:

- **Name**—Network designation
- **Prot**—IP protocol only
- **Int**—Name of the LAN interface this network runs on: atmnet:1, eth:1, eth:2, loopback, internal, slot:x/mod:y
- **State**—State of the network; Ena(bled) or Dis(abled)
- **Type**—*Static* (user-specified), *Auto* (default) or *Dynamic* network
- **Network address**—Address of the IP network

Syntax

```
list ip networks
```

Example

```
list ip networks
```

Related Commands

[add ip network](#)
[delete ip network](#)
[disable ip network](#)
[enable ip network](#)
[reconfigure ip network <network name>](#)
[set ip network <name>](#)
[show ip network <network_name> settings](#)

list ip pools This command displays the IP pools you configured with the add IP pool command. It lists the following information:

- **Name**—Pool designation
- **address**—Initial IP address and subnet mask of specified pool
- **Size**—Number of IP addresses you made available in the pool
- **InUse**—Number of IP addresses currently in use within the pool

- **State**—Conditional status of the IP pool. This value is either **public** or **private**
- **Route**—Indicates whether pool is being broadcast as a single network (aggregate) or separate networks (no_aggregate).
- **Status**—Indicates current condition of pool. Values displayed are as follows:
 - **Active**—Pool is available to assign user IP addresses from.
 - **Remove**—Pool size is being modified or the base address of the pool is being modified. No users can be assigned from the pool until operation is completed.
 - **Remove_pending**—Pool size is being modified and an active user is currently using a pool entry that needs to be removed. Users can be assigned from the pool in this state.
 - **Delete_pending**—Pool is being deleted but an active user has been assigned out of this pool and must wait until user hangs up to delete the pool. Users are not assigned from the pool in this state.

Syntax

```
list ip pools
```

Example

```
list ip pools
```

Related Commands

[add address_pool user](#)

[add ip pool](#)

[delete address_pool user](#)

[delete ip pool](#)

[enable ip address_pool_filtering](#)

[set ip pool](#)

list ip routes

This command displays all the statically defined IP routes that you previously defined using the add ip route command, as well as any routes learned via RIP and system-defined routes (loopback). This reflects information collected from the Forwarding Table.



Aggregate routes are not displayed by this command. See the [list ip pools](#) command for their display.

Syntax

```
list ip routes
```

- **Destination**—IP address that the route resolves to
- **Prot**—*LOCAL*, *RIP* or *NetMgr* (routes you added)

- **NextHop**—Address of the gateway used to reach this route
- **Metric**—Number of router hops away this route is from the system
- **Interface**—Interface that the route uses. Loopback, eth:1, eth:2, or slot:x/mod:y.

Example

```
list ip routes
```

Related Commands

[add ip route](#)

[delete ip route](#)

[set ip route <IP_hostname or network address>](#)

list ip source routes This command displays all the statically defined IP routes based on source routes that you previously defined using the `add ip source_route` command.

When source based addressing is enabled with the `enable ip source_address_routing` interface, the IP packets coming in on a static interface are looked up on a routing table based on the source address and routed accordingly. If source address lookup fails, the destination address is looked up failing which the default route is used.

Syntax

```
list ip source routes
```

Example

```
list ip source routes
```

list ip static_arp This command displays the static ARP table which lists all of the address resolution protocol (ARP) entries defined previously using the `add ip arp address` command.

Syntax

```
list ip static_arp
```

Example

```
list ip static_arp
```

list ipx networks This command displays the IPX networks that you previously defined using the [add ipx network](#) command. It lists the following information.

- **Name**—Designation you assigned this network
- **Prot**—Protocol; always IPX
- **Interface**—Interface each IPX network runs on
- **State**—Enabled or disabled
- **Type**—STATIC or DYNAMIC
- **Network address**—Network address of this IPX network

Syntax

Example

Related Commands

[add ipx network](#)

[delete ipx network](#)

[disable ipx network](#)

[enable ipx network](#)

[set ipx network](#)

[show ipx network <network name> settings](#)

[show ipx network <network_name> counters](#)

list ipx routes This command displays IPX routes you previously defined using the **add ipx route** command, plus the defined IPX nodes, including any IPX routes learned via RIP. It lists the following information.

- **Network address**—Network address of this route
- **Prot(ocol)**—Protocol used to find this route. Values displayed are **LOCAL**, **RIP**, **STATIC**, **NLSP**, or **OTHER**
- **NextHopNIC**—Network address of the next router (the next hop to the destination) or the MAC address for the local IPX nodes (on the LAN)., or the **ATM PVC**
- **Gateway**—Address of the gateway to this network
- **Metric**—Number of hops through routers this network is distant from
- **Ticks**—Estimated interval in eighteenths of a second for packet delivery to the remote network

Syntax

```
list ipx routes
```

Example

```
list ipx routes
```

Related Commands

[add ipx route](#)

[delete ipx route](#)

list ipx services This command displays IPX pool addresses previously defined with the [add ipx service](#) command. It lists the following information.

- **Name**—Name of the IPX service
- **NetNum**—Network number that the service is on
- **Node**—Name of the IPX node running the service
- **Socket**—Socket number of the service
- **Type**—Service type in hexadecimal format
- **Prot**—Protocol used to find this service. Values displayed are **SAP**, **LOCAL**, **NLSP**, **STATIC**, or **OTHER**
- **Metric**—Number of hops through routers to reach this service

Syntax

```
list ipx services
```

Example

```
list ipx services
```

Related Commands

[add ipx service](#)

[delete ipx service](#)

[delete ipx service_all](#)

list ipx static routes This command displays all IPX static routes previously defined using the add ipx route command.

- **Network address(es)**—Network address requiring this route
- **NextHopNIC**—Network address of the next router in the routing path
- **Gateway**—Address of the host you defined as the gateway
- **Metric**—Number of routers a packet must pass through to get to gateway
- **Ticks**—Delay, in hops, to reach the route's destination

Syntax

```
list ipx static routes
```

Example

```
list ipx static routes
```

list lan interfaces This command displays installed interfaces—Ethernet (eth:1, eth:2), along with its operational status, administration status, and interface index. If the interface is DOWN under Admin Status, you can use enable interface to try to bring it up. The command lists:

- **Name**—LAN interface name. eth:1 or eth:2
- **Oper Status**—Current operating status of the interface. Up or Down
- **Admin Status**—Permanently configured status of the interface. Up or Down

Syntax

```
list lan interfaces
```

Example

```
list lan interfaces
```

list ppp This command displays PPP bundles and links. When multiple physical links are combined to run multilink PPP (RFC 1717), the group of physical links is called a bundle. The second link (channel) will become active when the channel_expansion percentage has been exceeded. You can check the percentage using list ppp, and change it using the set network user ppp command.

- **Bundle Index**—Index number of the physical interface in the bundle
- **Link Index**—Index number in the list of links
- **Oper Status**—Current operational status of the link. Opened or Not Opened
- **Interface Name**—Slot and modem designation of interface belonging to this bundle/link

Syntax

```
list ppp
```

Example

```
list ppp
```

**set ip
application_source_
address**

This command specifies the source IP address (where packets exit) of a router card which has more than one Ethernet interface for IP routing or multi-home logical networks configured on the Ethernet and which needs to communicate that source address to an associated RADIUS or SYSLOG server. When configured (eth:1 or eth:2), the source address (of UDP packets) *overrides* both the internal IP address and *autoconfigured* IP system hosts address.

The router card Ethernet addresses range in importance as follows:

- Source IP address (highest priority)
- Internal IP address
- Default IP address (lowest priority)

When the IP address is configured at 0.0.0.0, this option is not set. The [show ip settings](#) command displays this configuration.

Syntax

```
set ip application_source_address [radius | syslog | igmp |  
l2tp_lac | ping | pptp_pac | traceroute | vtp] <IP_address>
```

Example

```
set ip application_source_address syslog 10.10.3.3
```

Related Commands

[set ip unnumbered link local address <IP address>](#) (for configuration of Ethernet IP addresses supplied to remote PPP or SLIP users when they dial up the router card)

set ip arp address This command changes or sets parameters for the specified IP address in the static ARP table.

Syntax

```
set ip arp address <IP address>
    access_mac_address <mac_addr>
    interface <interface_name>
    state [private | public]
```

Table 122 Set IP ARP Address Command Parameters Descriptions

Parameter	Description
ip_addr	The IP address entry for which you want to set parameters in the ARP table.
access_mac_address	The MAC address of the system that has the specified IP address.
interface	The interface with which to associate the specified IP address.
state	private—Only check for a static ARP entry for the interface receiving the ARP request. public—If there isn't a static ARP entry for the current interface, check the table to see if the IP address is set for all interfaces.

set ip defaultroute gateway This command sets the default route to the gateway.

Syntax

```
set ip defaultroute gateway <IP address or name>
```

Example

```
set ip defaultroute gateway 10.10.3.3
```

set ip defaultroute metric These commands reconfigure a backup default route. The commands change the address or metric of a *primary* default route with a gateway on the IP network configured on the first router card LAN interface (eth:1), and values for a *backup* default route with a gateway on the IP network configured on the second router card LAN interface (eth:2).

A default route gateway specified with a higher metric acts as the *primary* default route gateway and a second default route gateway with a lower metric acts as the *secondary* default route gateway.

If one Ethernet interface goes down, the default route gateway associated with that interface is disabled. If a second default route gateway associated with a still-alive interface exists, that gateway will be installed as the primary gateway. If the disconnected Ethernet interface is reconnected, the associated gateway will be re-installed.

Syntax

```
set ip defaultroute metric <hop count>
```

Table 123 Set IP Default Router Command Parameters Descriptions

Parameter	Description
<IP_address>	IP address of the gateway router.
metric	An integer representing how far away the default router is, in hops through other routers. The range is 1 to 15. The default is 1.

Related Commands

[add ip defaultroute gateway](#)

[delete ip defaultroute gateway](#)

set ip network <name>

This command configures the type of broadcast algorithm, the maximum size for reassembling fragmenting packets, the RIP password, RIP export metric, RIP policies, the routing metric and the routing protocol for the specified interface. The only required parameter for this command is <name>. All other parameters are optional. You can set all of them at once or one at a time. This command can only be used on IP networks previously defined using the `add ip network <network_name>` command. Use the `list ip networks` command to list the currently defined IP networks.

As activated by this command, routing is appropriate on a LAN segment where the default route gateway is *not* used because the router card dynamically adds discovered hosts to its Routing Table. Since the default is *none*, routing is not activated until you select `ripv1` or `ripv2`.



You must disable the IP network before setting these parameters. Use the `disable ip network` command or the `set ip network` command followed by the `reconfigure ip network` command. By issuing a `show ip network <name> settings` command, you can determine from the `Reconfigure Needed: field` whether a reconfigure was done.

Syntax

```
set ip network <IP address>
    broadcast_algorithm [bsd | ietf]
    reassembly_maximum_size <number>
    rip_authentication_key <string>
    rip_export_metric <0 to 15>
    rip_policies_update <rip_policies>
    routing_metric <1 to 16>
    routing_protocols [none | ripv1 | ripv2 | ospf]
```

RIP Policies—The following RIP policies are supported by the IP route:

- **Send Default**—*disabled* by default, causes router to advertise itself as the default router.
- **Send Routes**—enabled by default. Tells RIP to advertise (broadcast) its routes on the network every 30 seconds—is standard for a gateway router.
- **Send Subnets**—disabled by default. If this flag is on, only routes with the same network and with subnets on the same network are sent out the interface.
- **Accept Default**—disabled by default. Determines whether router accepts default route advertisements.
- **Split Horizon**—enabled by default. Records the interface over which it received a particular route and does not propagate its information about that route back over the same interface. This prevents network loops.
- **Poison Reverse**—disabled by default. Routes that were excluded due to the use of split horizon are instead *included* with infinite cost (16). The system continues to broadcast the route, but with an infinite cost.



In order to perform poison reverse, you must also enable split horizon.

- **Flash Update**—enabled by default. It is also known as “triggered update,” meaning routes that have their metrics modified will be advertised immediately, instead of waiting for the next scheduled broadcast.

The flags described on the next page are for backward compatibility with RIP version 1 when RIP version 2 is selected as the routing protocol.

- **Send Compatibility**—Controls the selection of destination MAC and IP addresses. It is enabled by default. When enabled, *broadcast* address is used; when disabled, *multicast* address is used.
- **RIP V1 Receive**—Controls the receipt of RIP version 1 updates. When RIP version 1 is the selected routing protocol, this policy is enabled by default, which means RIP version 1 packets are received. (When RIP version 2 is chosen, this policy is enabled by default, meaning RIP version 1 packets are received.)
- **RIP V2 Receive**—Controls receipt of RIP version 2 updates. When RIP v1 is the selected routing protocol, this policy is enabled by default, which allows RIPv1 packets to be received. When RIP version 2 is selected, this policy is enabled by default, allowing RIPv2 packets to be received. RIPv2 is backward compatible.
- **Silent**—This flag tells RIPv2 not to send updates. It is *disabled* by default.

Configure the following parameters.

Table 124 Set IP Network Command Parameters Descriptions

Parameter	Description
<network_name>	Designation of the IP network for which you want to set parameters. The limit is 32 ASCII characters.
broadcast_algorithm	Algorithm that determines which address is used in broadcasts to represent the entire network. Choices are: <ul style="list-style-type: none"> ■ IETF—the IETF standard: nnn.nnn.nnn.255 (default) ■ BSD—the BSD standard: nnn.nnn.nnn.000
reassembly_maximum_size	Maximum size IP datagram that the system will try to reassemble, when the datagram has been fragmented to fit in the network packet size. The default is 3464.
rip_authentication_key	ASCII string used for RIPv2 authentication.
rip_export_metric	Number of hops to advertise routes via this IP network. This value is set only when <i>RIPv1</i> or <i>RIPv2 routing_protocol</i> is selected. When the routing protocol is <i>none</i> , this value is automatically reset to the default: 0. The range is 0-15.
rip_policies_update	Allows user to enable or disable RIP policies. A keyword with a <i>no_</i> in front is used to disable the policy. Default policies are indicated by (D). <p>Note: For Poison Reverse to work properly, Split Horizon must also be enabled.</p> SEND_DEFAULT NO_SEND_DEFAULT(D) SEND_ROUTES(D)NO_SEND_ROUTES SEND_SUBNETSNO_SEND_SUBNETS(D) ACCEPT_DEFAULTNO_ACCEPT_DEFAULT(D) SPLIT_HORIZON(D)NO_SPLIT_HORIZON POISON_REVERSENO_POISON_REVERSE(D) FLASH_UPDATE(D)NO_FLASH_UPDATE SEND_COMPAT(D)NO_RIPV1_SEND RIPV1_RECEIVE(D)NO_RIPV1_RECEIVE RIPV2_RECEIVE(D)NO_RIPV2_RECEIVE SILENT (default is disabled)
routing_metric	Sets routing metric (number of hops between the router card and its destination) for use on IP network. Metric is set when the <i>routing_protocol</i> is configured as <i>ripv1</i> or <i>ripv2</i> . When <i>routing_protocol</i> is changed to <i>none</i> , the metric is changed back to the default value of 1. A metric value of 16 effectively shuts off RIP on that interface. The configured metric value is globally saved and retrieved after system reboot when the save all command is issued. <p>A metric is considered the cost to use an interface with lower metrics corresponding to better, more direct routes. When employing primary and backup routers with RIP enabled, you can set a low metric on the primary router interface (eth:1) and a higher metric on the backup router interface (eth:2). Range 1-16. The default is 1.</p>
routing_protocol	Sets routing protocol to be used on IP network. Choices are: none, RIP version 1, RIP version 2 or OSPF. The default is None.

Related Commands

[add ip network](#)
[delete ip network](#)
[disable ip network](#)
[enable ip network](#)
[list ip networks](#)
[reconfigure ip network <network name>](#)
[show ip network <network_name> settings](#)

**set ip route
 <IP_hostname or
 network address>**

This command modifies the IP route created using the add ip route command.

Syntax

```
set ip route <IP hostname or network address>
    gateway <host name or IP address>
    metric <1 to 15>
```

Table 125 Set IP Router Command Parameters Descriptions

Parameter	Description
<IP hostname or IP network address>	IP address or host name of the remote destination, in the format <i>nnn.nnn.nnn.nnn</i> , entered <i>with</i> or <i>without</i> a mask specifier. The mask specifier can be 'A', 'B', 'C', or 'H' (host), or a numeric value from 8 to 30 (32 if a host) that describes the number of one bits in the mask. You can also specify the netmask in the <i>xxx.xxx.xxx.xxx</i> format. If you do not specify a mask, the system will self-generate it (based on the network address) for all routes except <i>host</i> routes, for which you <i>must</i> specify a mask.
gateway	Host name or IP address of the next hop to the specified IP network address
metric	Number of hops the destination is removed from the specified IP network address. The range is 1 to 15.

Related Commands

[add ip route](#)
[delete ip route](#)
[list ip routes](#)

set ip routing This command sets global parameters for IP routing on the specified IP router address which serves as the gateway to an autonomous system.

Syntax

```
set ip routing
    autonomous_system_number <number>
    metric_maximum_entries <number>
    rip_flags <metrics, send_request>
    router_id <IP_address>
```



IP routing must be disabled before setting these values.

An autonomous system is a connected group of networks run by one or more network operators which has a single and clearly defined routing policy. An autonomous system number is a unique identifier for such a system, but is not currently supported by the router card. The *maximum* number of IP routes that can be contained in the Routing Table is 10.

Table 126 Set IP Routing Command Parameters Descriptions

Parameter	Description
autonomous_system_number	Value associated with a protocol not currently supported. Disregard this value. The range is 1-65535.
metric_maximum_entries	Most next hop entries the Next Hop Hash Table can hold. The default is 512. The range is 256-65535.
router_id	IP address of the router card. If value not specified, the system will take a user-configured internal IP address for this value, or the eth:1 value if no internal value is specified.
rip_flags	Flags indicate at which level a RIP instance is disabled or configured. Choices are: <ul style="list-style-type: none"> ■ Metrics—Specifies how to increment metrics using RFC 1058. ■ Send_request—Sends a RIP request for routing data when an interface first comes up.

Related Commands

[disable ip routing](#)

[enable ip routing](#)

set ip source_based_routing This command enables or disables source based routing on the specified interface.

Syntax

```
set ip source_based_routing <interface_name>
    enabled [no | yes]
```

Table 127 Set IP Source Based Routing Command Parameters Descriptions

Parameter	Description
interface_name	The name of the interface to which to apply this command.
enabled	no—Do not allow source based routing on this interface. yes—Allow source based routing on this interface.

set ip source route This command changes parameters in the routing table for the specified IP source route.

Syntax

```
set ip source route <IP name or net addr>
    gateway <ip_name_or_addr>
    metric <metric>
```

Table 128 Set IP Source Route Command Parameters Descriptions

Parameter	Description
ip_name_or_net_addr	The network name or IP address of the source route to be changed
gateway	The network name or IP address of the gateway to which IP datagrams with the specified source address should be routed.
metric	This specifies how many hops it is to the specified gateway.

**set ip unnumbered_link
local_address <IP
address>**

This command specifies the local IP address supplied to unnumbered PPP or SLIP users when they dialup the router card. When the IP address is configured as 0.0.0.0, this option is *not* set. If the local IP address is not set using this command, the *internal* IP address of the router card will be used as the local IP address. If an internal IP address also is not set, the IP address of one of the Ethernet interfaces (eth:1/eth:2) will be used as the local IP address.



This command allows multiple router cards to report the same LAN address to users for LAN-to-LAN routing purposes. Be careful not to configure an unreachable address as the reported address for the router card or unpredictable actions may occur. Be aware that the router cards sharing a LAN address will answer a ping from a client but the answer may not return from the expected router card.

Use this command to:

- Select a specific local address from an *internal* IP address or *Ethernet* IP addresses when more than one of the Ethernet interfaces are configured and/or an internal IP address is configured.
- Set an *arbitrary* IP address as the *reported* local address for PPP/SLIP unnumbered links. Note that in this case, no IP route will be added in the router card for this arbitrary local IP address. This address is not considered as an IP address of the router card.

Local and remote IP addresses are configured on a *user* basis with [add ip network](#), [set dialout user](#) and [set network user](#) commands. The [show ip settings](#) command displays this configuration.

Syntax

```
set ip unnumbered_link local_address <IP address>
```

Related Commands

[set ip application_source_address](#) (for information about configuring the router card Ethernet addresses for RADIUS and SYSLOG servers)

set ipx network This command sets configuration of the specified IPX network created with the [add ipx network](#) command.

Syntax

```
set ipx network <network name>
    delay_ticks <number>
    diagnostics [disable | enable]
    maximum_learning_retries <number>
    netbios [enable | disable]
    netbios_cache_timer <seconds>
    netbios_max_hops <number>
    netbios_name_cache [disable | enable]
    packet_maximum_size <number>
    rip [auto_off | auto_on | on | off]
    rip_age_multiplier <number>
    rip_broadcast [enable | disable]
    rip_gap_timer <number>
    rip_packet_size <number>
    rip_periodic [disable | enable]
    rip_receive [disable | enable]
    rip_update_interval <number>
    sap [auto_off | auto_on | on | off]
    sap_age_multiplier <number>
    sap_broadcast [enable | disable]
    sap_gap_timer <number>
    sap_nearest_replies [on | off]
    sap_packet_size <number>
    sap_periodic [enable | disable]
    sap_receive [disable | enable]
    sap_update_interval <number>
```

Table 129 Set IPX Network Command Parameters Descriptions

Parameter	Description
<network_name>	Designation of the IPX network. Maximum size: 32 characters.
delay_ticks	Interval in number of ticks it takes to reach this IPX network. The default is 1 for LAN networks, 40 for WAN networks. The range is 0 -65535.
diagnostics	Whether or not to send diagnostic packets to this IPX network. The default is enabled.
maximum_learning_retries	Number of times this network will resend packets to learn its directly connected neighbors. The default is 0.

Table 129 Set IPX Network Command Parameters Descriptions (continued)

Parameter	Description
netbios	Whether to support NetBIOS on dial-out IPX networks. The default is enabled.
netbios_cache_timer	Interval a NetBIOS system is kept in the cache. The default is 60 seconds.
netbios_name_cache	Whether or not to cache a list of the other NetBIOS systems on this IPX network. The default is disabled.
netbios_max_hops	Maximum number of hops this network will make to locate a NetBIOS system. The default is 8. The range is 0—65535.
packet_maximum_size	Maximum size packet this IPX network supports. Max size: 1600 bytes
rip	Turns RIP: on, off, auto_on or auto_off for this network. The default is On.
rip_age_multiplier	Number to multiply the rip_update_interval by, to obtain the value for the aging out the entries in the RIP database. The default is 3.
rip_broadcast	Enables/disables RIP broadcasts. The default is enabled.
rip_gap_timer	Interval the system waits between sending RIP packets. The default is 1.
rip_packet_size	Size of RIP packets. The default is 446 bytes.
rip_periodic	Enables/disables sending of RIP periodic updates. The default is enabled.
rip_receive	Allows the router to stop learning RIP updates from a given IPX Network.
rip_update_interval	How often RIP should send periodic updates. The range is 1-500 seconds. The default is 60 seconds.
sap	Turns SAP: on, off, auto_on or auto_off for this network. The default is On.
sap_age_multiplier	Number to multiply the sap_update_interval by, to obtain the value for aging out entries in the SAP database. The range is 1-1080. The default is 3.
sap_broadcast	Enables, disables SAP broadcasts. The default is enabled.
sap_gap_timer	Interval the system should wait between sending SAP packets. The default is 1.
sap_nearest_replies	Whether or not SAP will look for its nearest neighbors. The default is YES.
sap_packet_size	Size of SAP packets. The default is 510 bytes.
sap_periodic	Enables/disables sending of SAP periodic updates. The default is enabled.
sap_receive	Allows the router to stop learning SAP updates from a given IPX network.
sap_update_interval	How often RIP should send periodic updates. The range is 1-500 seconds. The default is 60 seconds.

Related Commands

[add ipx network](#)

[delete ipx network](#)

[disable ipx network](#)

[enable ipx network](#)

[list ipx networks](#)

[show ipx network <network name> settings](#)

[show ipx network <network name> counters](#)

show ip settings This command displays system-wide IP information.

Syntax

```
show ip settings
```

- IP System Host address—IP address of the router card
- IP Forwarding—*Enable* or *Disable* forwarding of IP packets
- IP Address Pool Filtering—*Enable* or *Disable* pool filtering
- IP Address Pool Round Robin—Whether IP addresses are allocated via the round robin method or not.
- Source Ip Address Filter—When enabled, the router card will filter and discard all upload packets that do not have a source IP address that matches the one negotiated.
- IP Multicast Proxy Interface—the router card's IGMP proxy interface. If configured, the interface on which any groups learned or joined on other interfaces will be joined. This interface can be either the router card's Eth:1, Eth:2, or slot:x/mod:y port or the username associated with the remotely attached host. The default is None.
- IP Multicast Heartbeat Status—Indicates whether multicast heartbeat is Enabled or disabled. The default is disabled.
- IP Multicast Heartbeat Interface—The interface on which multicast traffic for the specified group is monitored: *eth:1*, *eth:2*, or *slot:x/mod:y*. The default is None.
- IP Multicast Heartbeat Group—The IP address of the multicast group being monitored.
- IP Multicast Heartbeat Time—The interval, in seconds, multicast traffic is being monitored. The default is 60 seconds. The range is 0-65535.
- IP Multicast Heartbeat Window—The number of periods (in time values) multicast traffic is being monitored. The default is 5. The range is 0-255.
- IP Multicast Heartbeat Threshold—The interval during which multicast traffic is not received after which an SNMP trap is issued. The default is 3. The range is 0-65535.

- IP Source address for RADIUS—The router card's source IP address (where packets exit) supplied to an associated RADIUS server
- IP Source address for SYSLOG—The router card's source IP address (where packets exit) supplied to an associated SYSLOG server
- IP Local address for Unnumbered Links—Ethernet IP address supplied to remote PPP or SLIP users when they dialup the router card
- IP source address for IGMP—If configured, all IGMP packets sent from any of the router card's interfaces will use this address as its source address. The default is 0.0.0.0.
- IP source address for PPTP—The router card's source IP address (where packets exit) associated with a PPTP connection.
- IEA Next Hop Routing—When enabled, if the configured next hop routing interface is unreachable, the router card can still direct user traffic using other routing information, including the default gateway.
- IEA Send Unsolicited Proxy Arp—Shows whether it is enabled or disabled.
- IEA Force Next Hop Route—If enabled, forces the system to disconnect the dial-in user if the configured IEA next hop routing interface is unreachable. When disabled, and the configured next hop routing interface is unreachable, the router card can still direct user traffic using other routing information, including the default gateway.
- IP proxy ARP for all dialin addresses—Shows whether or not the sending of a proxy ARP response for dial-in IP addresses even if they are not part of the LAN is enabled or disabled. This feature is disabled by default.
- Send ICMP Host Unreachable for Pool—Enables and sends ICMP unreachable for pool addresses. This feature is disabled by default.
- IP source address for PING—The router card's source IP address that is used as the source of PING messages sent.
- IP source address for Trace Route—The router card's source IP address that is used as the source of traceroute messages sent.
- IP Respond to Directed Broadcast packets—Enables the router card to respond to ICMP requests or generate ICMP error messages for packets coming to a directed broadcast address of its networks.

show ip network settings

This command displays parameter settings for the IP network.

Syntax

```
show ip network settings
```

- Interface—Interface this IP network runs on.
- Network address—Network address and subnet mask of the router card.

- Frame Type—Frame type used by the router card. Choices: ETHERNET_II or SNAP.
- Mask—Subnet mask of the router card.
- Station—Station address of the router card.
- Broadcast Algorithm—Broadcast algorithm used for this network. The default is IETF.
- Max Reassembly Size—Maximum packet size allowed to be reassembled from fragments.
- IP Routing Protocol—Routing protocol used. The default is None.
- IP RIP Routing Policies—Routing policies used by RIP.
- IP RIP Authentication Key—Text string used for RIPv2 authentication.
- Status—Enabled, ACTIVE, INACTIVE, Disabled
- Reconfigure Needed—TRUE or FALSE. When displaying the value TRUE, this setting notifies the administrator that the network should be reinitialized in order for a newly configured parameter to take effect. Using the reconfigure command allows the network to automatically re-enable without having to manually disable and enable the network. The value FALSE indicates no network editing has occurred and no reconfiguration is required.
- IP Routing Metric—Routing metric configured for this network. Range 1-16. The default is 1.

Related Commands

[add ip network](#)

[delete ip network](#)

[disable ip network](#)

[enable ip network](#)

[list ip networks](#)

[reconfigure ip network <network name>](#)

[set ip network <name>](#)

**show ip network
<network_name>
settings**

This command displays the parameter settings for the specified network.

Syntax

```
show ip network <network name> settings
```

Example

```
show ip network chicago setting
```

show ip routing settings

This command displays parameter settings for the specified IP network. Statistics are gathered from parameters configured with [set ip routing](#).

Syntax

```
show ip routing settings
```

- IP Router Administrative Status — Whether status is enabled or not. The default is enabled.
- IP Static Remote Routes — Whether static routes are enabled or not. The default is enabled.
- LAN Host address — IP address of the router card.
- IP Autonomous System Number — System number assigned. The default is 1.
- IP Max Table Size — Maximum number of IP Routing Table entries allowed. The default is 1,415.
- IP Max Metric Entries — Maximum metric entries allowed. The default is 512.
- IP RIP — Whether RIP is enabled or not. The default is enabled.
- IP Number RIP Interfaces — Number of RIP interfaces.
- IP Number RIP Neighbors — Number of IP RIP neighbors.
- IP RIP Flags — Type of IP RIP flags enabled.

Example

```
show ip routing settings
```

show ip source_based_routing <interface_name>

This command displays the source IP address (where packets exit) of a router card which has more than one Ethernet interface for IP routing or multi-homed logical networks configured on the Ethernet.

Syntax

```
show ip source_based_routing <interface_name>
```

Example

```
show ip source_based_routing eth1
```

show ipx

This command displays settings for dynamic IPX networks. You can modify these values using the `set ipx system` command.

Syntax

```
show ipx
show ipx settings
```

- **Default Gateway** — Default IPX router address.
- **Name** — Designation for dynamic IPX networks.
- **Network Number** — Network number for dynamic IPX networks.
- **Max Open Sockets** — Maximum allowed number of open sockets to remote IPX networks.
- **Max Hops** — Maximum allowed hops to remote IPX networks.
- **Priority** — Preferred ranking of dynamic IPX networks.
- **Dynamic address Pool Begin** — Starting IPX address.
- **Number of Dynamic Pool Members** — Number of addresses to reserve for dynamic IPX address assignments.

Example

```
show ipx settings
```

show ipx network <network name> settings

This command displays parameter settings for the specified IPX network. You can modify most of these values using the set ipx network command.

Syntax

```
show ipx network <network name> settings
```

- **Interface** — Interface this IPX network uses. ETH:1 or ETH:2
- **Network address** — Network address of this IPX network.
- **Frame Type** — Frame type used by the interface (ETHERNET II, NOVELL_8023, SNAP, or LOOPBACK).
- **Maximum Packet Size** — Maximum allowable packet size for this IPX network. The default is 1500.
- **Status** — operational state of the network. The default is enabled.
- **Network Delay (ticks)** — Time in number of ticks it takes to reach this IPX network. The default is 1.
- **Network Learning Retries** — Number of times this network will resend packets to discover its directly connected neighbors.
- **Diagnostics** — Sending of diagnostic packets. The default is enabled.
- **NetBIOS** — Support. The default is enabled.
- **NetBIOS Name Caching** — Support. The default is DISABLED.
- **NetBIOS Cache Timer (sec)** — Interval. A NetBIOS system will be kept in the cache. The default is 60.
- **NetBIOS Maximum Hops** — Most hops this network will make to locate a NetBIOS system. The default is 8.
- **RIP State** — Status: ON, OFF, AUTO ON, or AUTO OFF. The default is ON.

- **RIP Pace** — Fastest pace, in packets per second, at which RIP packets may be sent on this circuit (*not settable via the CLI*).
- **RIP Update (sec)** — Interval, in seconds, after which RIP periodic updates are transmitted. The default is 60.
- **RIP Age Multiplier** — Number the *rip_update_interval* is multiplied by to obtain the *update* value. The default is 4.
- **RIP Max Packet Size** — Largest allowable size of a RIP packet. The default is 446.
- **RIP Broadcast** — Support. The default is enabled.
- **RIP Periodic** — Support. The default is enabled.
- **SAP State** — Support: ON or OFF. The default is ON.
- **SAP Pace** — Fastest pace, in packets per second, at which SAP packets may be sent on this circuit (*not settable via the CLI*). The default is 1.
- **SAP Update (sec)** — Interval, in seconds, after which SAP periodic updates are transmitted. The default is 60.
- **SAP Age Multiplier** — Number the *sap_update_interval* is to multiplied by to obtain the *update* value. The default is 4.
- **SAP Packet Size** — Greatest allowable size of a SAP packet. The default is 510.
- **SAP Broadcast** — Support. The default is enabled.
- **SAP Periodic** — Support. The default is enabled.
- **SAP Nearest Server Reply** — SAP seeks nearest neighbors: YES or NO. The default is YES.

Related Commands

[add ipx network](#)

[delete ipx network](#)

[disable ipx network](#)

[enable ipx network](#)

[list ipx networks](#)

[set ipx network](#)

[show ipx network <network_name> counters](#)

show ipx rip settings This command displays information about RIP for IPX.

Syntax

```
show ipx rip settings
```

- **State**—*ON* or *OFF*
- **Incorrect RIP Packets**—Number of RIP packets that do not make sense.

Example

```
show ipx rip settings
```

show ipx sap settings This command displays information about SAP for IPX.

Syntax

```
show ipx sap settings
```

- **State**—*ON* or *OFF*
- **Incorrect SAP Packets**—Number of SAP packets that do not make sense

Example

```
show ipx sap settings
```

Related Commands

[disable ipx sap network](#)

[enable ipx sap network](#)

[show ipx network <network name> settings](#)

add cross_connect This command adds and configures cross-connect parameters.

Syntax

```
add cross_connect <name>
```

```
peak <number>
```

```
vci1 <32 to 65535>
```

```
vci2 <32 to 65535>
```

```
vpi1 <0 to 255>
```

```
vpi2 <0 to 255>
```

Table 130 Add Cross_Connect Command Parameters Descriptions

Parameter	Description
<number>	Port number.
peak	The peak bandwidth for this PVC in kilobits/second. Default: 0 (bandwidth = 1/10 of interface speed).
vci1	Specified VCI for the PVC on Port1 to be connected. Range: 32-65535.

Table 130 Add Cross_Connect Command Parameters Descriptions

Parameter	Description
vci2	Specified VCI for the PVC on Port2 to be connected. Range: 32-65535.
vpi1	Specified VPI for the PVC on Port1 to be connected. Range: 0-255.
vpi2	Specified VPI for the PVC on Port2 to which the VCI1 value will be connected. Range: 0-255.

enable cross_connect This command enables ATM cross connections.

Syntax

```
enable cross_connect
```

Example

```
enable cross_connect
```

disable cross_connect This command disables ATM cross connections

Syntax

```
disable cross_connect
```

Example

```
disable cross_connect
```

list cross_connect This command lists current ATM cross connection statics.

Syntax

```
list cross_connect
```

Example

```
list cross_connect
```

show cross_connect This command shows the following statistics on the specified ATM cross connection.

Syntax

```
show cross_connect <name>
```

- **Cross Connect Name**—Designation of the cross connection to allow easy recognition and configuration on the router card.
- **Port1**—Number of Port1.
- **VPI1**—Specified VPI for the PVC on Port1 to be connected.
- **VCI1**—Specified VCI for the PVC on Port1 to be connected.

- **Port2**—Number of Port2.
- **VPI2**—Specified VPI for the PVC on Port2 to which the VCI1 value will be connected.
- **VCI2**—Specified VCI for the PVC on Port2 to be connected.
- **PCR**—The peak bandwidth for this PVC in kilobits/second.
- **Status**—The status of the cross connection, enabled or disabled.

DNS

add dns host This command adds the named host to the Local Host Table. When the system needs to resolve an address for an IP host name, the Local Host Table is checked first, before a request is sent to the remote DNS Name Server.

Syntax

```
add dns host <host name and domain name>
        address <IP address>
```

Table 131 Set Add DNS Host Command Parameters Descriptions

Parameter	Description
<host_name>	Designation of the local host. The limit is 32 ASCII characters.
address	IP address of a named host in xxx.xxx.xxx.xxx format.

Related Commands

[delete dns host](#)

[list dns hosts](#)

add dns server This command adds the IP address of a remote DNS server to the Domain Name Server Table. The preference number specifies the order DNS servers in this table are accessed, with 1 as the highest preference and 10 as the lowest. The first specified server is sent the IP Host Name to be resolved, first *with*, then *without* the default domain name (see *set dns domain_name* for more information about the default domain name). If that server cannot resolve the name, it is sent to the next specified server.



The router card will try to reach each configured host three times in round-robin fashion before issuing an error message. For instance, in the case of three off-line servers—A, B and C—the router card will admit failure only after trying to reach them one after the other, three times.

Syntax

```

add dns server <IP address>
    preference <priority_rating>
    name <server_name and domain_name>

```

Table 132 Add DNS Server Command Parameters Descriptions

Parameter	Description
<IP address>	IP address of a server in <i>nnn.nnn.nnn.nnn</i> format.
preference	Specifies the order in which name servers are used, with 1 as the highest priority. The range is 1-10.
name	Designation (optional) of the name server. The limit is 32 ASCII characters.

Related Commands

[delete dns server preference](#)
[list dns servers](#)
[set dns server preference](#)

delete dns cache This command removes an entry from the DNS Cache Table. The range is 0 to 65535.

Syntax

```
delete dns cache <number>
```

Example

```
delete dns cache 100
```

delete dns host This command deletes the specified host from the DNS Local Host Table. Use list DNS hosts to view the DNS Local Host Table. After deletion, requests for that host will be processed through a DNS server, instead of locally. Use list DNS servers to see which servers are defined.

Syntax

```
delete dns host <name>
```

Related Commands

[add dns host](#)
[list dns hosts](#)

delete dns ncache This command removes the specified entry from the DNS Negative Cache Table. The range is 0 to 65535.

Syntax

```
delete dns ncache <number>
```

Example

```
delete dns ncache 100
```

delete dns server preference This command removes the name server associated with that preference number (preferred rank: 1 [first] -10 [least]) from the table of accessible DNS servers.

Syntax

```
delete dns server preference <preference_number>
```

Related Commands

[add dns server](#)

[list dns servers](#)

[set dns server preference](#)

disable dns host_rotation This command disables the router card process of randomly choosing a primary IP address and up to eight alternates from the DNS cache.

Syntax

```
disable dns host_rotation
```

Example

```
disable dns host_rotation
```

Related Commands

[enable dns host_rotation](#)

disable dns round_robin This command disables the router card process of sequentially choosing a primary IP address and up to eight alternates from the DNS cache. Use the command to view the current setting.

Syntax

```
disable dns round_robin
```

Example

```
disable dns round_robin
```

Related Commands[enable dns round_robin](#)[show dns settings](#)

enable dns host_rotation This command enables the router card process of randomly choosing a primary IP address and up to eight alternates from the DNS cache. Use the show dns command to view the current setting.

Syntax

```
enable dns host_rotation
```

Example

```
enable dns host_rotation
```

Related Commands[disable dns host_rotation](#)[show dns settings](#)

enable dns round_robin This command enables the router card process of sequentially choosing a primary IP address and up to eight alternates from the DNS cache. Use the show dns command to view the current setting.

Syntax

```
enable dns round_robin
```

Example

```
enable dns round_robin
```

Related Commands[disable dns round_robin](#)[show dns settings](#)[enable dns host_rotation](#)

host <IP_host_name> This command returns an IP address for the specified host name by sending it to DNS for resolution. If the Domain Name has been specified using the [set dns](#) command, it will also be resolved; otherwise you must specify it as part of the name. This command requires either a DNS local host (add DNS host) or a DNS server entry (add DNS server) to resolve the name. This command is identical to the [resolve name](#) command.

```
Network Name: host.commworks.com
is resolved to address: 123.123.123.111
```

Syntax

```
host <IP address or host name>
```

Example

```
host commworks
```

list dns cache This command displays entries in the DNS Cache table.

Syntax

```
list dns cache
```

- **Number**—Row number in DNS Cache Table.
- **Pretty Name**—Name of the Resource Record in the cache which is identified in this row of the table. As described in RFC-1034, the owner of the record is the domain name were the resource record is found.
- **Class**—DNS class of the Resource Record in the cache which is identified in this row of the table.
- **Type**—DNS type of the Resource Record in the cache which is identified in this row of the table.
- **IP Address**—If the Type of the entry is listed as 1, the IP address of that entry is listed.
- **Source**—Host from which Resource Record was received, 0.0.0.0 if unknown.

Example

```
list dns cache
```

list dnis_connections This command displays the DNIS/ANI information for all of the active sessions.

Syntax

```
list dnis_connections
```

- **IfName**—Modem slot and interface of current connections
- **User Name**—Name of users currently connected
- **Type**—Current type of connections established on the modems. They include:
 - **On-demand**—User connection established for on-demand purposes
 - **Dial-back**—User connection established for callback purposes
 - **Continuous**—User connection established for continuous utilization
 - **Manual**—User connection established on the fly
 - **Timed**—User connection established for a particular interval
 - **ShrMod (Shared-modem)**—Dial-out user connection to a modem utilizing a login service (Telnet or rlogin) or NCSI. LED does not light until call is unhooked (amber) and connected (green). NCSI sessions using the port redirector display *None* as the DLL type.
 - **Dialin**—User connection established for dial-in purposes. LED lights *amber* when modem is unhooked, *green* when call is connected.
 - **Bond**—User connection utilizing bandwidth allocation
 - **Dedicated**—User connection established for a particular user
- **DLL**—Data link layer that the specified dial-in session is connected to: NONE, PPP, SLIP, SHELL, RL(O)G(I)N, TLNT, PING, ADMN, CL(EAR)TCP, L2TP, PPTP, TAP, PRMT
- **Calling Phone**—The calling phone number.
- **Called Phone**—The called phone number.

Example

```
list dnis_connections
```

list dns hosts This command displays the DNS local host and its IP address, which you configured using add dns host.

Syntax

```
list dns hosts
```

Example

```
list dns hosts
```

Related Commands

[add dns host](#)

[delete dns host](#)

list dns ncache This command displays entries in the DNS Negative Cache table.

Syntax

```
list dns cache
```

- **Number**—Row number in DNS Negative Cache Table.
- **Pretty Name**—Name of the Resource Record in the cache which is identified in this row of the table. As described in RFC-1034, the owner of the record is the domain name were the resource record is found.
- **Class**—DNS class of the Resource Record in the cache which is identified in this row of the table.
- **Type**—DNS type of the Resource Record in the cache which is identified in this row of the table.
- **Source**—Host from which Resource Record was received, 0.0.0.0 if unknown.

Example

```
list dns cache
```

list dns servers This command displays DNS Name Servers, which you configured using the `add dns server` command. It lists the following information:

- **Preference**—server priority for DNS service
- **Name**—your name for the server
- **address**—IP address of server
- **Status**—current status (ACTIVE, INACTIVE)

Syntax

```
list dns servers
```

Example

```
list dns servers
```

Related Commands

[add dns server](#)

[delete dns server preference](#)

[set dns server preference](#)

set dns This command sets the global parameters for DNS; both local DNS hosts ([list dns hosts](#)) and remote DNS servers ([list dns servers](#)), and DNS caching and negative caching parameters, in support of DNS host rotation for load balancing.

Syntax

```
set dns
    cache [enabled | disabled | clear]
    cache_maxttl <0 to 2147483>
    domain_name <string>
    ncache [enabled | disabled | clear]
    ncache_maxttl <0 to 2147483>
    number_retries <number>
    timeout <interval>
```

Table 133 Set DNS Command Parameters Descriptions

Parameter	Description
cache	Enables or disables DNS caching. Setting to CLEAR flushes the DNS cache. The default is disabled.
cache_maxttl	Maximum time in seconds DNS cache entries remain in the DNS cache before they're flushed. The range is 0 to 2147483.
domain_name	Default domain designation to be used if no domain is specified (by add dns server command) in the name to be resolved. For example: usr.com. The limit is 32 ASCII characters.
ncache	Enables or disables negative DNS caching. Setting to CLEAR flushes the DNS negative cache. The negative DNS cache contains entries the DNS server found to be in error. For example, if the host name abc.xyz.com doesn't exist, the DNS server will return a non-existent name error.
ncache_maxttl	Maximum time in seconds DNS negative cache entries remain in the DNS negative cache before they're flushed. The range is 0 to 2147483.
number_retries	Number of times the resolve name request will be sent to each Name Server if the server fails to respond to a request before the timeout period. The default is 1. The range is 1-5.
timeout	Interval in seconds to wait before deciding a request to a Name Server has timed out. Minimum interval and default is 5 seconds, maximum interval is 245 seconds.

Related Commands

[disable dns host_rotation](#)

[enable dns host_rotation](#)

[set login user](#)

set dns server preference This command redefines the name of a DNS, which you previously defined using the `add dns server` command. Use the `list dns servers` command to see the currently defined DNS servers.

Syntax

```
set dns server preference <number>
    name <server name and domain name>
    address <IP address>
```

Example

```
set dns server preference <number>
```

Table 134 Set DNS Server Preference Command Parameters Descriptions

Parameter	Description
preference <number>	Priority of the name server in name searches from 1 (highest) to 10 (lowest).
server name	Unique designation given to the DNS server. This field is optional, but is useful for keeping track of name servers. You can also supply the domain name. The limit is 32 ASCII characters.
address	IP address of the DNS server.

Related Commands

[add dns server](#)

[delete dns server preference](#)

[list dns servers](#)

show dns settings This command displays settings for all DNS servers.

Syntax

```
show dns settings
```

- **Domain Name**—default domain name to be used if no domain is specified in the name to be resolved.
- **Number Retries per Server**—number of times the resolve name request will be sent to each Name Server, if the server fails to respond to a request before the timeout period.
- **Timeout Period in Seconds**—number of seconds to wait before deciding a request to a Name Server has timed out.
- **Cache Max TTL**—Maximum Time-To-Live period in seconds for resource records in this cache.
- **Negative Cache Max TTL**—Maximum Time-To-Live period in seconds for negative cached authoritative errors.
- **Caching**—Indicates whether function is **enabled** or **disabled**.

- **Negative Caching**—Indicates whether function is **enabled** or **disabled**.
- **Host Rotation**—Indicates whether function is **enabled** or **disabled**.

Example

```
show dns settings
```

Related Commands

[set dns](#)

show dns cache This command displays an entry in the DNS Cache Table.

Syntax

```
show dns cache <1 to 65535>
```

- **Pretty Name**—Fully qualified name (resource record) the host connects to (at this row in the table). See RFC-1035, section 2.3.3 for more information.
- **Class**—DNS class of the resource record at this row in the table.
- **Type**—DNS type of the resource record at this row in the table.
- **TTL**—Time To Live period in seconds of the resource record.
- **Elapsed TTL**—Period in seconds since resource record was received.
- **DNS Server**—Host from which resource record was received, 0.0.0.0 if unknown.
- **Data**—RDATA portion of a cached RR. The value is in the format defined for the particular DNS class and type of the resource record. See RFC-1035, section 3.2.1 for more information.
- **(Error) Status**—Status column for the resolver cache table. Since only the agent (DNS resolver) creates rows in this table, the only values that a manager may write to this variable are Active and Destroy.

show dns ncache This command displays an entry (row) in the DNS Negative Cache Table.

Syntax

```
show dns ncache <1 to 65535>
```

- **Pretty Name**—Fully qualified name (resource record) the host connects to (at this row in the table).
- **Class**—DNS class of the resource record at this row in the table.
- **Type**—DNS type of the resource record at this row in the table.
- **TTL**—Time To Live period in seconds of the resource record.
- **Elapsed TTL**—Period in seconds since resource record was received.
- **DNS Server**—IP address of the fully qualified name.
- **Error Code**—Type of authoritative error indicated in the table. Types include:
 - **Nonexist(ant Name)**—authoritative name error.
 - **No Data**—authoritative response with no error and no relevant data.
 - **Other**—some other cached authoritative error. At present, no such errors are known to exist.
- **(Error) Status**—Status column for the resolver negative response cache table. Since only the agent (DNS resolver) creates rows in this table. Types include: **Active** and **Destroy**.

Frame Relay

add frame_relay pvc This command creates a Frame Relay Permanent Virtual Circuit (PVC) on top of the Frame Relay DLL added for the physical WAN interface. The PVC's DLCI value is a number supplied by your Telco. Depending on the LMI protocol selected for the Frame Relay DLL, the DLCI ranges from 16 to 991 for ANSI T1.617 Annex D and ITU Q.933 Annex A or from 16 to 1007 for LMI rev.1. Optionally, you can define the Administrative State of the PVC as enabled or disabled. The default for the enabled parameter is yes.

Syntax

```
add frame_relay pvc <pvc name>
    dlci <number>
    interface <interface name>
    enabled [yes | no]
```

When a PVC is created, the Frame Relay stack creates a *logical* interface as its representation. The logical interface name is defined as *interface_name/pvc_name*. The name can consist of up to 32 ASCII characters. For example; wan:1/boston. This logical interface instance is used to define the

Related Commands

[delete frame_relay pvc](#)
[disable frame_relay pvc](#)
[enable frame_relay pvc](#)
[set frame_relay pvc <pvc_name>](#)
[show frame_relay pvc <pvc_name> settings](#)
[show frame_relay pvc <pvc_name> counters](#)

add frame_relay ptmp_pvc_group

This command adds multipoint pvc groups.

Syntax

```
add frame_relay ptmp_pvc_group <net_name>
```

Related Commands

[list frame_relay ptmp_pvc_group](#)

list frame_relay ptmp_pvc_group

This command lists pvc group statics for specified pvc group.

Syntax

```
list frame_relay ptmp_pvc_group <net name>
```

Related Commands

[add frame_relay ptmp_pvc_group](#)

show frame_relay ptmp_pvc_group <net name> counters

This command shows frame relay multipoint pvc group counters.

Syntax

```
show frame_relay ptmp_pvc_group <net name> counters
```

Related Commands

[list frame_relay ptmp_pvc_group](#)

**show frame_relay
ptmp_pvc_group <net
name> settings**

This command shows the following statics for the specified group:

- **Index**—The index number of the multipoint group.
- **Name**—The name of the multipoint group.
- **Status**—Whether multipoint group is up or down.
- **PVCs**—The number of PVCs configured for this group.
- **RowStatus**—Indicates the present status of the row.
 - active
 - notInService
 - notReady
 - createAndGo
 - createAndWait

Syntax

```
show frame_relay ptmp_pvc_group <net name> settings
```

Related Commands

[list frame_relay ptmp_pvc_group](#)

**show frame_relay pvc
<net name> settings**

This command shows the following statics:

- **Interface**—The interface name for the frame relay to which the PVC is being added.
- **DLCI**—The datalink connection identifier associated with this PVC, supplied by your Telco.
- **PVC Name**—The unique designation of the permanent virtual circuit, maximum of 32 characters. White space in the name must be enclosed by double quotes. For example: "wan:1/boston west".
- **Oper State**—The operational state of the frame relay, which could be enabled, disabled, or down.
- **Admin. State**—Whether the frame relay is active or not in service.

Syntax

```
show frame_relay pvc <net name> settings
```

show frame_relay pvc This command displays frame relay pvc counters.
<net name> counters

Syntax

```
show frame_relay pvc <net name> counters
```

add datalink This command creates a Frame Relay Data Link Layer (FR DLL) on top of the
frame_relay interface physical WAN interface (for example, wan:1). Optionally, it defines the
<interface_name> Administrative State of the FR DLL as enabled or disabled. Name can be up to
32 ASCII characters. The default for the enabled parameter is yes.

Syntax

```
add datalink frame_relay interface <interface_name>  
    enabled [yes | no]
```

Related Commands

[delete datalink frame_relay interface](#)

[disable datalink frame_relay interface](#)

[enable datalink frame_relay interface.](#)

**delete datalink
frame_relay interface**

This command removes the Frame Relay Data Link Layer defined on top of the physical WAN interface.

Syntax

```
delete datalink frame_relay interface <interface_name>
```

Related Commands

[add datalink ppp user <username>](#)

[disable datalink frame_relay interface](#)

[enable datalink frame_relay interface](#)

delete frame_relay pvc

This command removes the specified PVC.

Syntax

```
delete frame_relay pvc <pvc_name>
```

Related Commands

[add frame_relay pvc](#)

[disable frame_relay pvc](#)

[enable frame_relay pvc](#)

[set frame_relay pvc <pvc_name>](#)

[show frame_relay pvc <pvc_name> settings](#)

[show frame_relay pvc <pvc_name> counters](#)

add framed_route user

Framed Route specifies the static route, or specific set of routers that the connection must take.

Syntax

```
add framed_route user <user name> ip_route <IP address> gateway  
<IP address>
```

Example

```
add framed_route user bsmith ip_route 10.10.3.3 gateway 10.10.10.1
```

**delete framed_route
user**

This command deletes the framed route user you created with the add frame_route user command.

Syntax

```
delete framed_route user <name>  
ip_route <IP name or address>
```

Related Commands[add framed_route user](#)

disable frame_relay pvc This command disables the administrative and operational state of the specified PVC.

Syntax

```
disable frame_relay pvc <pvc_name>
```

Related Commands[add frame_relay pvc](#)[delete frame_relay pvc](#)[enable frame_relay pvc](#)[set frame_relay pvc <pvc_name>](#)[show frame_relay pvc <pvc_name> settings](#)[show frame_relay pvc <pvc_name> counters](#)**disable datalink
frame_relay interface**

This command disables the Administrative and operational state of the Frame Relay DLL created on top of the physical WAN interface. This causes all PVCs associated with this interface to go down.

Syntax

```
disable datalink frame_relay interface <interface name>
```

Related Commands[add datalink ppp user <username>](#)[delete datalink frame_relay interface](#)[enable datalink frame_relay interface](#)**enable datalink
frame_relay interface**

This command enables the administrative state of the Frame Relay DLL created on top of the physical WAN interface.

Syntax

```
enable datalink frame_relay interface <interface name>
```

Related Commands[add datalink ppp user <username>](#)[delete datalink frame_relay interface](#)[disable datalink frame_relay interface](#)[list frame_relay](#)

enable frame_relay pvc This command enables the administrative state of the specified PVC.

Syntax

```
enable frame_relay pvc <pvc name>
```

Related Commands

[add frame_relay pvc](#)

[delete ip source route](#)

[disable frame_relay pvc](#)

[set frame_relay pvc <pvc_name>](#)

[show frame_relay pvc <pvc_name> settings](#)

[show frame_relay pvc <pvc_name> counters](#)

list frame_relay This command displays Frame Relay configuration—the defined Frame Relay DLLs and associated Frame Relay PVCs defined on top of them. It lists the following information:

Syntax

```
list frame_relay
```

- **Interface Name**—Designation of the router card Frame Relay interface.
- **PVC Name**—Designation of the PVC.
- **DLCI**—Data Link Connection Interface Number supplied by Telco (if over Frame Relay network) or internally.
- **Operational Status**—The *current* operating state of the data link. Status is determined by the success or failure of the LMI message exchange with the Frame Relay switch, the WAN interface state and the Administrative Link State. The possible states are:
 - **Ready**—Ready to pass data packets on the PVC.
 - **Wait For Driver**—Interface waiting for the driver to be ready (e.g., the physical interface is not ready).
 - **Recovery**—The DLL is recovering from the Down state.
 - **Down**—DLL procedures indicate the DLL is not able to operate.
 - **Disabled**—Cannot pass data packets on the DLL because the Administrative Link State is disabled.
- **Administrative Status**—The *desired* state of the Frame Relay interface or PVC and whether they are:
 - **Enabled**—Ready to pass data packets
 - **Disabled**—Not ready to pass data packets

Example

```
list frame_relay
```

set frame_relay conformance This command sets conformance test suite option to conform to either conformance test suite (Idacom or Sprint). The default is idacom.

Syntax

```
set frame_relay conformance [idacom | sprint]
```

Example

```
set frame_relay conformance idacom
```

set frame_relay traps This command configures whether SNMP traps are enabled or disabled. The default is off.

Syntax

```
set frame_relay traps [on | off]
```

Example

```
set frame_relay traps on
```

set frame_relay trap_min_interval This command configures the interval in msec between trap messages.

Syntax

```
set frame_relay trap_min_interval <number>
```

Example

```
set frame_relay trap_min_interval 1
```

set frame_relay interface This command configures the Frame Relay DLL created on top of the physical WAN interface as specified by the *interface_name* parameter.

Syntax

```
set frame_relay interface <interface name>
    access_rate <number>
    error_threshold <number>
    full_enquiry_interval <number>
    management_type [ansi | itu | lmi | no_lmi]
    max_supported_pvc <max_supported_pvc>
    monitored_events <number>
    mtu <number>
    polling_interval <number>
    pvc_learning [on | off]
```

Table 135 Set Frame_Relay Interface Parameters Descriptions

Parameter	Description
access_rate	Speed of the physical WAN interface expressed in bits per second (bps). If this value is set to 0, the Frame Relay DLL uses an interface speed value provided by the WAN interface driver as an <i>access_rate</i> value. The range is 0 to 8192000 . The default is 1544000 bps .
error_threshold	Maximum number of unanswered LMI Status Enquiries the router card accepts before declaring the DLL inactive. The range is 1 to 10 . The default is 3 .
full_inquiry_interval	Period that elapses before a LMI Full Status Enquiry message is issued. The range is 1 to 255 . The default is 6 .
management_type	Link Management Interface (LMI) protocol used between user and network equipment. Choices are: <ul style="list-style-type: none"> ■ ANSI—ANSI T1.617 Annex D ■ ITU—ITU Q.933 Annex A ■ LMI—LMI rev. 1 ■ NO LMI—Link Management Interface protocol turned off. This selection sets up a Frame Relay direct connection between two peers, without the need for a Frame Relay switch. The condition of the Frame Relay DLL is determined based on physical WAN interface signaling. <p>The default is ANSI.</p>

Table 135 Set Frame_Relay Interface Parameters Descriptions (continued)

Parameter	Description																
max_supported_pvc	<p>Maximum number of PVCs that can be created on this DLL.</p> <p>The upper boundary for this value depends on two parameters, MTU size and currently selected MANAGEMENT_TYPE. By default this value is set to its maximum, based on the combination of these two parameters. The following formula is used to calculate the MAX_SUPPORTED_PVCS maximum value:</p> $\text{max_value} = (\text{MTU} - \text{LMI_header_size}) / \text{PVCS_IE_size}$ <p>Where MTU is current MTU value (default 1600) and the values of LMI_header_size and PVCS_IE_size depending on MANAGEMENT_TYPE selection are shown below along with the computed max_value:</p> <table border="1"> <thead> <tr> <th>MANAGEMENT_TYPE</th> <th>LMI_header_size</th> <th>PVCS_IE_size</th> <th>max_value</th> </tr> </thead> <tbody> <tr> <td>ANSI</td> <td>14</td> <td>5317</td> <td></td> </tr> <tr> <td>ITU</td> <td>13</td> <td>5317</td> <td></td> </tr> <tr> <td>LMI</td> <td>13</td> <td>8198</td> <td></td> </tr> </tbody> </table> <p>If MANAGEMENT_TYPE is set to NO_LMI the maximum max_value is 976.</p>	MANAGEMENT_TYPE	LMI_header_size	PVCS_IE_size	max_value	ANSI	14	5317		ITU	13	5317		LMI	13	8198	
MANAGEMENT_TYPE	LMI_header_size	PVCS_IE_size	max_value														
ANSI	14	5317															
ITU	13	5317															
LMI	13	8198															
monitored_events	<p>Number of status polling intervals over which an error threshold is counted. If, for a specified number of events, the Frame Relay DLL receives the specified number of threshold errors, the Frame Relay DLL is declared to be inactive. The range is 1 to 10. The default is 4.</p>																
mtu	<p>Maximum Transfer Unit on the Frame Relay DLL. It defines the maximum number of bytes the Frame Relay DLL attempts to transmit or receive through its physical interface in a single frame. The range is 260 to 2048 bytes. The default is 1600.</p>																
polling_interval	<p>Period, in seconds, between successive LMI Status Inquiry messages sent by the Frame Relay DLL. The range is 5 to 30 seconds. The default is 10.</p>																
pvc_learning	<p>Turns PVC Learning on or off. When On, the Frame Relay DLL adds a new PVC or removes the existing PVC <i>dynamically</i>, based on information received in the LMI Status frame. The default is off.</p>																

Related Commands

[show frame_relay interface <interface_name> settings](#)

set frame_relay pvc This command configures the specified Frame Relay PVC.
<pvc_name>

Syntax

```
set frame_relay pvc <pvc name>
    attached_to_group <ptmp_group_name>
    bc_max <number>
    bc_min <number>
    be <number>
    becn_cmp <number>
    becn_monitoring [on | off]
    cir <number>
    cir_monitoring [on | off]
    detached_from_group
```

Table 136 Set Frame_Relay PVC Command Parameters Descriptions

Parameter	Description
attached_to_group	Attach the pvc to the designated Point To MultiPoint (PTMP) group
bc_max	Upper boundary of the Committed Burst Size (Bc) parameter which defines the maximum amount of data the PVC offers to the network, under normal conditions, during an internally set (non-configurable) time interval. The range is 0 to 8192000 bits. The default is 256000.
bc_min	Lower boundary of the Bc parameter which defines the maximum amount of data the PVC offers to the network, under normal conditions, during a time interval Tc. The range is 0 to 8192000 bits. The default is 128000.
be	Excess Burst Size (Be) parameter, which defines the maximum allowed amount of data, by which the PVC can exceed Bc during a time interval Tc. The range is 0 to 8192000 bits. The default is 0.
becn_cmp	Backward Explicit Congestion Notification (BECN) Congestion Monitoring Period (CMP), which defines a interval when the PVC monitors a number of received BECN events. The range is 1 to 100 seconds. The default is 10.
becn_monitoring	Turns BECN Monitoring On or Off. If turned On, the PVC monitors the <i>BECN</i> bit of the Q.922 header in received data packets. If the number of events where the BECN bit is set exceed the number of events where the BECN bit is cleared during the <i>becn_cmp</i> monitoring period, the <i>Bc</i> value is gradually decreased toward the <i>bc_min</i> value. In the opposite case, it is gradually increased toward the <i>bc_max</i> value. If turned Off, the PVC does not attempt to control the congestion notification information. The default is Off.
cir	Committed Information Rate (CIR), which defines the information transfer rate which the network is committed to transfer under normal conditions. The range is 0 to 8192000 bps. The default is 256000.
cir_monitoring	Turns CIR Monitoring On or Off. If turned On, the PVC monitors the amount of data transmitted through the physical interface and restricts this according to CIR rules. If turned Off, the PVC does not attempt to control outgoing data traffic. The default is On.
detached_from_group	Detach the pvc from the Point To MultiPoint (PTMP) group to which it is attached.

Related Commands

[add frame_relay pvc](#)

[delete frame_relay pvc](#)

[disable frame_relay pvc](#)

[enable frame_relay pvc](#)

[show frame_relay pvc <pvc_name> settings](#)

[show frame_relay pvc <pvc_name> counters](#)

**show frame_relay
interface
<interface_name>
settings**

This command displays the configuration of the DLL created on top of the physical WAN interface as specified by the *interface_name* parameter.

Syntax

```
show frame_relay interface <interface name> settings
```

- **Administrative Link State**—The *desired* state of the data link and whether it is:
 - **Enabled**—Enabled to pass data packets on the PVC.
 - **Disabled**—Disabled to pass data packets on the PVC.
- **Operational Status**—The *current* operating state of the data link. Status is determined by the success or failure of the LMI message exchange with the Frame Relay switch, the WAN interface state and the Administrative Link State. The possible states are:
 - **Ready**—Ready to pass data packets on the PVC.
 - **Wait For Driver**—Interface waiting for the driver to be ready (e.g., the physical interface is not ready).
 - **Recovery**—The DLL is recovering from the Down state.
 - **Down**—DLL procedures indicate the DLL is not able to operate.
 - **Disabled**—Cannot pass data packets on the DLL because the Administrative Link State is disabled.
- **Address Format**—The format of the address field in the encapsulated frame (q922).
- **Address Length**—Displays the length of the Frame Relay ITU Q.922 header. The only valid setting is **Two Octets**.
- **LMI Protocol Type**—The specified Link Management Interface Protocol used between the use and network equipment. Choices are:
 - **ANSI**—ANSI T1.617 Annex-D
 - **ITU**—ITU Q.933 Annex-A
 - **LMI**—LMI REV1
 - **NO LMI**—No LMI configured

- **Polling Interval T391/T1 [sec]**—Period, in seconds, between successive LMI Status Enquiry messages sent by the DLL.
- **Full Enquiry N391/N1**—Period that elapses before a LMI Full Status Enquiry message is issued.
- **Error Threshold N392/N2**—Maximum number of unanswered LMI Status Enquiries the router card accepts before declaring the Frame Relay DLL disconnected.
- **Monitored Events N393/N3**—Number of status polling intervals over which an error threshold is counted. If, for a specified number of events, the DLL receives the specified number of threshold errors, the DLL is declared to be disconnected.
- **Maximum Supported PVCs**—Limit of PVCs allowed on this interface as dependent on the MTU and LMI protocol type specified. At default MTU of 1600 bytes and LMI protocol type of ANSI T1.617Annex-D, the Maximum Supported number of PVCs is: **317**.
- **New PVC Learning**—Indicates this feature is **On** or **Off**. When On, the DLL adds a new PVC or removes the existing PVC *dynamically*, based on information received in the LMI Status frame.
- **Multicast**—Whether the specified is using a multicast service or not.
- **Maximum Transfer Unit [bytes]**—Maximum number of bytes the DLL tries to transmit/receive through its physical interface in a single frame.
- **Access Rate [bits/sec]**—Speed of the physical WAN interface in bits per seconds. If set to 0, the Frame Relay DLL uses an interface speed value provided by the WAN interface driver as an Access Rate value.

**show frame_relay pvc
<pvc_name> settings**

This command displays the configuration of the specified Frame Relay PVC.

Syntax

```
show frame_relay pvc <pvc_name> settings
```

- **Administrative Status**—The *desired* state of the Frame Relay PVC and which of the following states it is in:
 - **Enabled**—Enabled to pass data packets.
 - **Disabled**—Disabled to pass data packets.
- **Operational Status**—The *current* operational state of the Frame Relay PVC and which of the following states it is in:
 - **Up**—Ready to pass data packets.
 - **Down**—Not ready to pass data packets.
- **DLCI**—Data Link Connection interface supplied by Telco (if over Frame Relay network) or internally.
- **Type**—PVC type. Either:
 - **Static**—PVC configuration is defined by the administrator.
 - **Dynamic**—PVC configuration is learned from the Frame Relay network.
- **Multicast Type**—The network broadcast type supported. Currently supports Unicast.
- **CIR Monitoring**—Indicates whether this feature is **ON** or **OFF**. If ON, the PVC monitors the amount of data transmitted through the physical interface and restricts this according to CIR rules. If OFF, the PVC does not try to control the outgoing data traffic.
- **CIR [bits/sec]**—Committed Information Rate—the packet transfer rate, in bits per second, the network is committed to deliver under normal conditions.
- **Bc Maximum [bits]**—Upper boundary of the Committed Burst Size (Bc) or maximum amount of data the PVC may offer to the network, under normal conditions, during an internally set time interval (Tc).
- **Bc Minimum [bits]**—Lower boundary of the Committed Burst Size or maximum amount of data the PVC may offer to the network, under normal conditions, during an internally set time interval.
- **Bc Current [bits]**—Present Committed Burst Size value.
- **Be [bits]**—Excess Burst Size (Be) or maximum allowed amount of data by which the PVC can exceed the Committed Burst Size during an internally set time interval.
- **Tc [msec]**—A time interval used by the Congestion Avoidance Procedure to calculate CIR.
- **BECN Monitoring**—Indicates whether this feature is **ON** or **OFF**. If ON, the PVC monitors the BECN bit of the *Q.922 header* in received data packets. If the number of events where the BECN bit is set exceed the number of

events where the BECN bit is cleared during the *BECN CMP* monitoring period, the *Bc* value is gradually decreased towards the *Bc Minimum* value. In the opposite case, it is gradually increased towards the *Bc Maximum* value. If OFF, the PVC does not try to control the congestion notification information.

- **BECN CMP [sec]**—Backward Explicit Congestion Notification (BECN) Congestion Monitoring Period (CMP) defines a time interval when the PVC monitors a number of received BECN events.

Related Commands

[add frame_relay pvc](#)

[delete frame_relay pvc](#)

[disable frame_relay pvc](#)

[enable frame_relay pvc](#)

[set frame_relay pvc <pvc_name>](#)

[show frame_relay pvc <pvc_name> counters](#)

show frame_relay stack This command displays Frame Relay stack information.

Syntax

```
show frame_relay stack
```

- **Conformance**—Sets Conformance type, either Idacom or Sprint. More specifically, shows conformance test suite option currently set up for the router card Frame Relay stack.
- **SNMP**—Whether SNMP traps are on or off.
- **Interval Between Traps [msec]**—Time interval in msec between trap messages.

Example

```
show frame_relay stack
```

```
show datalink
frame_relay interface
<interface_name>
settings
```

This command displays the configuration of the DLL created on top of the physical WAN interface as specified by the *interface_name* parameter.

Syntax

```
show datalink frame_relay interface <interface_name> settings
```

It lists the following information:

- **Administrative Link State**—The *desired* state of the data link and whether it is:
 - **Enabled**—Enabled to pass data packets on the PVC.
 - **Disabled**—Disabled to pass data packets on the PVC.
- **Operational Status**—The *current* operating state of the data link. Status is determined by the success or failure of the LMI message exchange with the Frame Relay switch, the WAN interface state and the Administrative Link State. The possible states are:
 - **Ready**—Ready to pass data packets on the PVC.
 - **Wait For Driver**—Interface waiting for the driver to be ready (e.g., the physical interface is not ready).
 - **Recovery**—The DLL is recovering from the Down state.
 - **Down**—DLL procedures indicate the DLL is not able to operate.
 - **Disabled**—Cannot pass data packets on the DLL because the Administrative Link State is disabled.
- **Address Format**—The format of the address field in the encapsulated frame (q922).
- **Address Length**—Displays the length of the Frame Relay ITU Q.922 header. The only valid setting is **Two Octets**.
- **LMI Protocol Type**—The specified Link Management Interface Protocol used between the user and network equipment. Choices:
 - **ANSI**—ANSI T1.617 Annex-D
 - **ITU**—ITU Q.933 Annex-A
 - **LMI**—LMI REV1
 - **NO LMI**—No LMI configured
- **Polling Interval T391/T1 [sec]**—Period, in seconds, between successive LMI Status Enquiry messages sent by the DLL.
- **Full Enquiry N391/N1**—Period that elapses before a LMI Full Status Enquiry message is issued.
- **Error Threshold N392/N2**—Maximum number of unanswered LMI Status Enquiries the router card accepts before declaring the Frame Relay DLL disconnected.
- **Monitored Events N393/N3**—Number of status polling intervals over which an error threshold is counted. If, for a specified number of events,

the DLL receives the specified number of threshold errors, the DLL is declared to be disconnected.

- **Maximum Supported PVCs**—Limit of PVCs allowed on this interface as dependent on the MTU and LMI protocol type specified. At default MTU of 1600 bytes and LMI protocol type of ANSI T1.617 Annex-D, the Maximum Supported number of PVCs is: **317**.
- **New PVC Learning**—Indicates this feature is **On** or **Off**. When On, the DLL adds a new PVC or removes the existing PVC *dynamically*, based on information received in the LMI Status frame.
- **Multicast**—Whether or not the specified is using a multicast service.
- **Maximum Transfer Unit [bytes]**—Maximum number of bytes the DLL tries to transmit/receive through its physical interface in a single frame.
- **Access Rate [bits/sec]**—Speed of the physical WAN interface in bits per seconds. If set to 0, the Frame Relay DLL uses an interface speed value provided by the WAN interface driver as an Access Rate value.

ICMP

This section covers Internet Control Message Protocol (ICMP) commands of the CLI.

disable icmp router_advertise

This command disables the router card-generated router advertisements multicast on the same LAN segment as the router card.

Syntax

```
disable icmp router_advertise
```

Example

```
disable icmp router_advertise
```

Related Commands

[enable icmp router_advertise](#)

[show icmp settings](#)

enable icmp router_advertise

This command enables the router card-generated router advertisements multicast on the same LAN segment as the router card.

Syntax

```
enable icmp router_advertise
```

Example

```
enable icmp router_advertise
```

Related Commands

[disable icmp router_advertise](#)

[show icmp settings](#)

disable icmp logging This command disables display of the Internet Control Message Protocol (ICMP) to the SYSLOG server. Use `show icmp` to view edits. ICMP is disabled by default.

Syntax

```
disable icmp logging
```

Related Commands

[enable icmp logging](#)

[show icmp](#)

show icmp This command displays ICMP settings.

Syntax

```
show icmp
```

Example

```
show icmp
```

show icmp settings This command displays incoming login-access information including whether ICMP Logging and ICMP Router Advertise are enabled. You can turn multicasting of ICMP router advertisements on or off with [enable icmp router advertise](#) or [disable icmp router advertise](#).

Syntax

```
show icmp settings
```

Example

```
show icmp settings
```

Related Commands

[enable icmp router advertise](#)

[disable icmp router advertise](#)

MPIP

delete mpip client This command deletes the Multilink PPP client you created with the add mpip client command.

Syntax

```
delete mpip client <IP_address>
```

Example

```
delete mpip client 10.10.3.3
```

Related Commands

[add mpip client](#)

[list mpip clients](#)

[set mpip client](#)

delete mpip server This command deletes the Multilink PPP server you created with the add mpip server command.

Syntax

```
delete mpip server <IP_address>
```

Example

```
delete mpip server 10.10.3.4
```

Related Commands

[add mpip server](#)

[list mpip servers](#)

[set mpip client](#)

Multicasting

set ip multicast heartbeat This command configures multicast monitoring for a specified multicast *group* or *interface*.

Syntax

```
set ip multicast heartbeat
    interface <interface_name>
    group <ip_multicast_address>
    time <interval>
    threshold <number>
    window <number>
```

Table 137 Set IP Multicast Heartbeat Command Parameters Descriptions

Parameter	Description
<interface_name>	The interface on which to monitor multicast traffic for the specified group: eth:1 , eth:2 , slot:x/mod:y , or username
group	The IP address of the multicast group to monitor.
time	The interval, in seconds, to monitor multicast traffic. The range is 0 to 65535 . The default is 60 .
threshold	The interval during which multicast traffic is not received after which an SNMP trap is issued. The range is 0 to 65535 . The default is 3 .
window	The number of periods (in <i>time</i> values) to monitor multicast traffic. The range is 0-255 . The default is 5 .

Example

```
set ip multicast heartbeat
```

Related Commands

[enable ip multicast_heartbeat](#)
[disable ip multicast_heartbeat](#)
[show ip settings](#)

set ip multicast proxy interface The value for <interface_name> can be in the form Eth:1, Eth:2, slot:x/mod:y or username.

Multicast addresses that are joined or learned on the specified interface are joined on the proxy interface that is configured with this command.

Syntax

```
set ip multicast proxy interface <interface_name>
```

Related Commands

[set ip igmp \[eth:1 | eth:2 | slot:x/mod:y\]](#)

IGMP

join ip igmp <IP_multicast_address>

This command adds a member to this multicast address group. Entries are added to the IGMP Cache Table. Use the [list interfaces](#) command to view assigned interface names.

Syntax

```
join ip igmp <IP_multicast_address>
      interface [eth:1 | eth:2 | slot:x/mod:y]
```

Related Commands

[leave ip igmp <IP multicast address>](#)

leave ip igmp <IP multicast address>

This command removes a member from this multicast address group configured with the [join ip igmp <IP multicast address>](#) command. Entries are deleted from the IGMP Cache Table.

Syntax

```
leave ip igmp <IP multicast address>
      interface <interface name>
```

Related Commands

[join ip igmp <IP_multicast_address>](#)

list ip igmp

This command displays configured IGMP *interfaces*, their associated *multicast addresses*, and IGMP *status*.

Syntax

```
list ip igmp
```

- **Interface**—The Ethernet (**eth:1**, **eth:2**) or modem interface (**slot:x/mod:y**) to which the IGMP multicast address is mapped.
- **Multicast address**—An IP address assigned from the standard range of recognized addresses identifying an IGMP group. The range is **224.0.0.0-239.255.255.255**.
- **Status**—Description of how the specified multicast address joined the group. Status types may be single or combined. The types are:
 - **Self**—Multicast address group joined by the router card.
 - **Learned**—Multicast address group discovered by the router card (non-router card join).

- **Proxy**—Multicast address group connected to another interface on the router card.

Example

```
list ip igmp
```

set ip igmp [eth:1 | eth:2 | slot:x/mod:y]

This command Specifies Internet Group Management Protocol (IGMP) settings to configure IP multicast groups. the router card performs IGMP forwarding; the present release does not support IGMP routing protocols such as PIM and DVMRP.

Syntax

```
set ip igmp [eth:1 | eth:2 | slot:x/mod:y]
max_response_time <1-10 seconds>
multicast_forwarding [enabled | disabled]
multicast_proxy [enabled | disabled]
query_interval <5-65,535 seconds>
robustness <1-5>
routing [enabled | disabled]
version <1-2>
```

Table 138 Set IP IGMP Command Parameters Descriptions

Parameter	Description
<interface_name>	The interface on which IGMP is enabled: eth:1, eth:2 or slot:x/mod:y
max_response_time	The interval a host has to respond to the IGMP query. The default is 10. The range is 1-10 seconds.
multicast_forwarding	Multicast packets are forwarded when enabled. The default is disabled.
multicast_proxy	Multicast addresses that are joined or learned on the specified interface are joined on the proxy interface that is configured with the set ip multicast proxy interface command. The default is Disabled.
query_interval	The frequency at which IGMP Host-Query messages are sent on the specified interface. The default is 125.
robustness	Tuning parameter for expected packet loss on a subnet. If packet loss on a subnet is expected to be high, robustness may be increased. The range is 1-5. The default is 2.
routing	Will attempt to become the IGMP querier on this interface. The default is Disabled.
version	The version of IGMP running on this interface. This object can be used to configure a router capable of running either version. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN. The default is 2.

show ip igmp [eth:1 | eth:2 | slot:x/mod:y]

This command displays IP multicast settings for the specified interface.

Syntax

```
show ip igmp [eth:1 | eth:2 | slot:x/mod:y]
```

- **IGMP Interface**—Network interface of the router card. **Eth:1, Eth:2** or **slot:x/mod:y**
- **Query Interval**—Period, in seconds, IGMP Host-Query messages are sent on this interface. The default is **125 seconds**.
- **Max Response**—Maximum time a host has to respond to query requests on this interface. The default is **10 seconds**.
- **Version**—The version of IGMP running on this interface. The default is **Version 2**.
- **Querier**—Address of the IGMP Querier on the IP subnet to which this interface is attached.
- **Joins**—Number of times a group membership has been added on this interface—the number of times an entry for this interface has been added to the IGMP Cache Table. It indicates the amount of IGMP activity over time.
- **Robustness**—Setting for expected packet loss on a subnet. Default is **2**.
- **Groups**—Current sum of multicast groups active on this interface.
- **Routing**—If enabled, indicates that the router card will try to become a querier on this interface. If disabled, indicates the router card will act as an IGMP host and only report multicast groups it joins. The default is **Disabled**.
- **Multicast Forwarding**—Indicates if multicast packets will be received and transmitted on this interface. The default is **Disabled**.
- **Multicast Proxy**—If enabled, indicates any multicast groups joined or learned on this interface will also be joined on the interface configured as the multicast proxy interface. The default is disabled.
- **IGMP Short Packets**—Sum of IGMP short packets received on the specified interface.
- **IGMP Bad Checksum**—Sum of IGMP packets received with bad checksum on the specified interface.
- **Queries Received**—Sum of IGMP queries received on the specified interface.
- **Reports Received**—Sum of IGMP reports received on the specified interface.
- **Reports For Known Groups Received**—Sum of IGMP reports for known groups received on the specified interface.
- **Wrong Version Reports Received**—Sum of IGMP reports received with the wrong IGMP version number on the specified interface.
- **Reports Sent**—Sum of IGMP reports sent on the specified interface.

OSPF and Policy-Based Routing

This section covers Open Shortest Path First (OSPF) and policy-based routing commands of the CLI.

add ospf cryptographic_key <key_id>

This command creates an encrypted OSPF password for the specified interface. Each key is identified by the *interface* and associated *key id*. An interface may have multiple keys active at any one time. This enables smooth transition from one key to another. Each key has four time constants associated with it which can be expressed in terms of a time-of-day clock, or in terms of a router's local clock (e.g., number of seconds since last reboot).

Syntax

```
add ospf cryptographic_key <key_id>
    interface <ip_address or if_index>
    shared_key <password>
    start_accept <date.time>
    start_generate <date.time>
    stop_generate <date.time>
    stop_accept <date.time>
```

Table 139 Add OSPF Cryptographic Key Command Parameters Descriptions

Parameter	Description
key_id	Secret key identifier used to create the message digest appended to the OSPF packet. Key Identifiers are unique per-interface. The range is 1-255.
interface	IP address or interface index of this OSPF interface.
shared_key	An alphanumeric string. The maximum size is 16 characters.
start_accept	The time the router card will start accepting packets that were created with the configured key. For smooth key transition, <i>Start Accept</i> should be less than <i>Start Generate</i> . The default is Current time and date.
start_generate	The time the router card will start using the configured key for packet generation. The default is <i>Start accept</i> time plus 10 minutes.
stop_generate	The time the router card will stop using the key for packet generation. If <i>stop generate</i> and <i>stop accept</i> are left unspecified, the key's lifetime is infinite. For smooth key transition, <i>stop generate</i> should be less than <i>stop accept</i> . This parameter may be set manually to a value of infinity. The default is infinity.
stop_accept	The time the router card will stop accepting packets that were created with the given key. If <i>stop generate</i> and <i>stop accept</i> are left unspecified, the key's lifetime is infinite. This parameter may be set manually to a value of infinity. The default is infinity.



When a new key replaces an old key, the Start Generate time for the new key must be less than or equal to the Stop Generate time of the old key.

Date.time takes the form of DD-MMM-[YY]YY.HH:MM:SS. The valid range of years is 1997 through 2036. If only the date portion is specified, the time portion

is set to 0:0:0. If only the time portion is specified, the date portion is set to the current date.



*The parameters **stop_generate** and **stop_accept** will accept the value **infinity** in place of a date.time entry. If no value is entered, the default value for these parameters is **infinity**.*

To achieve smooth key transition, start_accept should be less than start_generate and stop_generate should be less than stop_accept. If stop_generate and stop_accept are left unspecified, the key's lifetime is infinite. When a new key replaces an old key, the start_generate time for the new key must be less than or equal to the stop_generate time of the old key.

Related Commands

[delete ospf cryptographic_key](#)

[list ospf cryptographic_key](#)

[set ospf cryptographic_key](#)

[show ospf cryptographic_key](#)

add ospf receivepolicy

This command creates an OSPF import policy that can filter ASEs from the routing table. Also use this command to affect how ASEs are accepted into the routing table.

When the action for the receivepolicy is set to accept, the routing_preference parameter is used to separate routes into groups that lead to the same destination. These groups are based on the protocol that generated the route. Choose the appropriate parameter (pref0, pref1, pref2, or pref3) depending on the preferred route. A lower preference value indicates a better route. For example, pref0 has a lower preference than pref1. If two routes have the same routing preference, then the route with the lower cost metric is used. It is important to remember that although a route assigned pref3 appears in the routing table, the route is never used to determine how to forward a packet. Essentially, a pref3 route is not used to forward packets.

Typically, both static routes and routes generated by RIP get assigned a routing preference equivalent to pref 1 (or OSPF external type 1 routes). Conversely, OSPF internal routes are preferred over RIP-generated or static routes.



An OSPF receive policy only affects an ASE when it is received. Once an ASE is in the LSDB (Link State Database) changing or adding a receive policy has no effect on the ASE.



*Setting the **routing_preference** parameter to a value of **pref3** is equivalent to setting the **action** parameter to a value of **ignore**. If the **action** parameter is set to a value of **ignore**, the **routing_preference** value has no effect. Changing the **action** parameter to a value of **accept** at a later time puts the stored **routing_preference** value into effect.*

Syntax

```

add ospf receivepolicy <network_address/ mask>
    action [accept | ignore]
    routing_preference [pref0 | pref1 | pref2 | pref3]

```

Table 140 Add OSPF Receivepolicy Command Parameters Descriptions

Parameter	Description
network_address/ mask	Required. The network address and mask describes the network match range. An external route of an ASE whose most significant bits match the portion of the policy's network address defined by the mask will be received or not (depending on the action specified in the routing table). The mask defines the number of consecutive bits, starting from the most significant bit to the least significant bit, that must match. The mask may be specified as a value from 8 to 32, or alternatively be entered in the format of an IP address class (A, B or C). No mask entry will result in a default mask being generated that matches the class of the specified network address.
action	Required. Configures whether to accept or ignore the specified route.
routing_preference	When the action for this receivepolicy is set to accept, you can specify the preferred route as one of the following: <ul style="list-style-type: none"> 0—Selects a routing preference equivalent to OSPF internal routes. 1—Selects a routing preference equivalent to OSPF external type 1 routes. 2—Selects a routing preference equivalent to OSPF external type 2 routes. 3—Signifies that the route is not used.

Related Commands

[`delete ospf receivepolicy <network_address/ mask>`](#)

[`list ospf receivepolicy`](#)

[`set ospf receivepolicy <network_address/ mask>`](#)

[`show ospf receivepolicy <network_address>`](#)

add ospf sendpolicy

This command creates a send (route leak) policy for the given destination. Send policies are used to define the set of autonomous system external routes to be redistributed into the OSPF domain.



When a send policy is added or modified the routing table is fully scanned automatically for a route and send policy match. This requires no user intervention. If a match is found and an ASE does not exist a new ASE is generated. If a match is found and an ASE exists and parameters have changed in its associated send policy the ASE is re-originated with the modified information.



Adding a local send policy for a local route associated with an interface that has OSPF enabled will have no affect.



*If the user record for a dial-in user has routing protocols set to **none**, and the ASBR functionality has been enabled, the user will automatically be advertised without a send policy.*

A framed user (a dial-in, point-to-point connection from a host) will automatically be advertised without a send policy.

Syntax

```
add ospf sendpolicy <network_address/ mask>
    action [advertise | do_not_advertise]
    metric <0 to 16777215>
    metric_type [type_i | typeii]
    source [local | rip | remote]
    tag <0 to 2147483647>
```

Table 141 Add OSPF Command Parameters Descriptions

Parameter	Description
network_ address/mask	Required. The network address and mask describes the network match range. An external route of an ASE whose most significant bits match the portion of the policy's network address defined by the mask will be sent or not (depending on the action specified in the routing table). The mask defines the number of consecutive bits, starting from the most significant bit to the least significant bit, that must match. The mask may be specified as a value from 8 to 32, or alternatively be entered in the format of an IP address class (A, B or C, or H). No mask entry will result in a default mask being generated that matches the class of the specified network address.
action	Required. Configures whether to redistribute (advertise) or block (not advertise) the specified route.
metric	Optional. Selects the metric value to be placed in an ASE. Setting this to 0 reads the metric value associated with a route contained in the routing table. Any other value (1-16777215) is used as the metric value that is placed in an ASE. The default is 0. The range is 0-16777215.

Table 141 Add OSPF Command Parameters Descriptions

Parameter	Description
metric_type	Optional. Configures the type of cost associated with external routes. Type 1 metrics represent the total cost of all steps (internal and external) between a source and a destination. Type 2 metrics represent only the cost of the external path to the destination.
source	Required. Route source including local and remote static routes, and routes learned via RIP. Note: When a host net mask is specified the source can not be set to local. This safeguard is in place to prevent overwriting a route with a subnet mask (e.g. 1.2.3.0/C) in another router with one that has a host net mask (e.g. 1.2.3.0/H), and cause that router to lose information on how to forward to the subnet (1.2.3.0/C, for example).
tag	Optional tag. Values range from 0 to 2147483647.

Related Commands[delete ospf sendpolicy](#)[list ospf sendpolicy](#)[set ospf sendpolicy](#)[show ospf sendpolicy](#)**show ospf sendpolicy**
<IP address> source

This command displays local, remote, or RIP OSPF information.

Syntax

```
show ospf sendpolicy <ip net address> source <local, remote, rip>
```

The following information is displayed.

- **ID**—The 32-bit integer uniquely identifying an area.
- **Type**—The area's support for determining if the type is Stub or Transit. If configured as Stub, the area will not support importing of AS external link-state advertisements. Transit denotes the area can support importing AS external link-state advertisements.
- **Status**—The status of the OSPF interface. Enabled denotes the area is in an active state. Disabled denotes the area is in an inactive state; either the area was administratively disabled or OSPF was globally disabled.

**delete ospf
cryptographic_key**

This command removes a MD5 cryptographic key created with the `add ospf cryptographic_key` command. Note that you can only delete a key whose status is *NotInService*.

Syntax

```
delete ospf cryptographic_key <key_id>
    interface <ip_address or if_index>
```

Related Commands

[add ospf cryptographic_key <key_id>](#)

[list ospf cryptographic_key](#)

[set ospf cryptographic_key](#)

[show ospf cryptographic_key](#)

**delete ospf
default_area**

This command deletes the previously configured default area and all associated OSPF interfaces, causing the *default_area_id* to revert back to its default value of 0.0.0.0.

Syntax

```
delete ospf default_area
```

Example

```
delete ospf default_area
```

Related Commands

[disable ospf area](#)

[enable ospf area](#)

[set ospf area](#)

[set ospf default_area_id](#)

[show ospf area <area_id> settings](#)

**delete ospf
receivepolicy
<network_address/
mask>**

This command removes the specified OSPF receivepolicy.

Syntax

```
delete ospf receivepolicy <network_address/ mask>
    source [local | rip | remote]
```

Table 142 Delete OSPF Command Parameters Descriptions

Parameter	Description
network_address/mask	The network address and mask describes the network match range.
source	Route source including local and remote static routes, routes learned via RIP.

Related Commands

[add ospf receivepolicy](#)

[list ospf receivepolicy](#)

[set ospf receivepolicy <network_address/ mask>](#)

[show ospf receivepolicy <network_address>](#)

delete ospf sendpolicy This command removes the specified OSPF sendpolicy.

Syntax

```
delete ospf sendpolicy <network_address/mask>
    source [local | rip | remote]
```



Deleting a send policy in an ASBR will cause any ASEs that were previously advertised under that policy by the ASBR to be flushed from the OSPF domain.

Table 143 Delete OSPF Command Parameters Descriptions

Parameter	Description
network_address/mask	The network address and mask describes the network match range.
source	Route source including local and remote static routes, routes learned via RIP.

Related Commands

[add ospf sendpolicy](#)

[list ospf sendpolicy](#)

[set ospf sendpolicy](#)

[show ospf sendpolicy](#)

disable ospf This command disables the administrative status of OSPF in the router card, effectively disabling the default OSPF area and all its associated OSPF interfaces. Disabling OSPF removes all routes learned by OSPF from the routing table and disables all associated timers.

Syntax

```
disable ospf
```

Example

```
disable ospf
```

Related Commands

[enable ospf](#)

[show ospf global settings](#)

disable ospf area This command administratively disables the OSPF area. The AreaID used should be the configured *default_area_id*, or 0.0.0.0. It is specified in dotted decimal notation.

Syntax

```
disable ospf area <area_ID>
```

Related Commands

[delete ospf default_area](#)

[enable ospf area](#)

[set ospf area](#)

[set ospf default_area_id](#)

[show ospf area <area_id> settings](#)

disable ospf interface This command administratively disables the OSPF interface.

Syntax

```
disable ospf interface <IP_address or IF_index>
```

Related Commands

[enable ospf interface](#)

[set ospf interface](#)

[show ospf interface <IP address or IF index> settings](#)

enable ospf This command enables the administrative status of Open Shortest Path First (OSPF) protocol in the router card, making the protocol operational. Unless otherwise configured, OSPF runs with default values as defined in RFC1850. If the OSPF is not explicitly configured, the OSPF router is set to the IP address of either the first broadcast interface or the configured internal network. See [disable ospf](#), [show ospf global counters](#), [show ospf global settings](#) and other OSPF commands throughout this manual for more information.

Syntax

```
enable ospf
```

Related Commands

[disable ospf](#)

[show ospf global counters](#)

[show ospf global settings](#)

enable ospf area This command administratively enables the default OSPF area. The *area_ID* used should mirror the configured *default_area id*, or 0.0.0.0.

Syntax

```
enable ospf area <area_ID>
```

Related Commands

[delete ospf default_area](#)

[disable ospf area](#)

[set ospf area](#)

[set ospf default_area_id](#)

[show ospf area <area_id> settings](#)

enable ospf interface This command administratively enables the OSPF interface.

Syntax

```
enable ospf interface <IP_address or IF_index>
```

Related Commands

[disable ospf interface](#)

[set ospf interface](#)

[show ospf interface <IP address or IF index> settings](#)

list ospf This command displays the specified ospf information.

Syntax

```
list ospf
  area
  lsdb type <lsa_type>
```

Table 144 List OSPF Command Parameters Descriptions

Parameter	Description
area	Displays ip address of the ospf area.
lsdb type	Displays the link-state database (lsdb) type for the OSPF router.

Example

```
list ospf area
```

list ospf cryptographic_key This command displays the status of all cryptographic keys created with add ospf cryptographic_key.

Syntax

```
list ospf cryptographic_key
```

It lists the following information:

- **IfIPAddr/IfInd**—IP address or interface index of the OSPF interface associated with this cryptographic key.
- **Id**—Key ID of this cryptographic authentication key.
- **Status**—Operational status of this key. There are two possible values. These include Active and NotinService. An Active status means that this key is currently in use for OSPF packet authentication. A NotinService status means the key is not in use for the OSPF interface identified.



If no cryptographic key has been configured for an OSPF interface, the default Cryptographic key with key_id = 0 will be used for authentication. This default key can not be deleted and cannot be displayed by the list or show commands. The lifetime of the default key is infinite.

Related Commands

[add ospf cryptographic_key <key_id>](#)
[delete ospf cryptographic_key](#)
[set ospf cryptographic_key](#)
[show ospf cryptographic_key](#)

list ospf host This command displays all OSPF hosts active in the default area.

Syntax

```
list ospf host
```

It lists the following information:

- **Host IP**—IP address of directly connected hosts.
- **Metric**—Cost of sending data to this host connection.
- **Area ID**—32-bit integer uniquely identifying the area to which the host is connected.

list ospf interface This command displays configuration information for all OSPF interfaces.

Syntax

```
list ospf interface
```

The following information is listed:

- **IfIpAddr/IfIns**—Specifies the interface identifier, either the IP address associated with the interface, or the address list interface ID.
- **AreaID**—Identifies the area associated with a router's interface.
- **IfType**—Indicates the interface type, either Broadcast (BC), Point-to-Point (PToP), Point to Multipoint (PToMP), or No Broadcast Multi-Access (NBMA).
- **AdminStat**—Shows administrative status, either enabled meaning OSPF packets can send/receive, or DISABLED meaning no OSPF packets can send/receive. For example, DISABLED would apply if the administrator is debugging or changing parameters.
- **IfState**—Indicates interface state, possible values include the following:
 - DOWN
 - LOOPBACK
 - Point-to-Point
 - Designated Router (DsgRtr)
 - Backup DsgRtr
 - Other DsgRtr
- **Metric**—A number indicating how long it will take to pass packets.



*If you disable and then enable an IP network on an interface when the OSPF link is physically disconnected, the admin state of the OSPF interface is wrongly reported as **disabled** by the **list ospf interface** command.*

When the physical connection is re-made it automatically comes up, the Admin state is set to **enabled**, and the OSPF interface forms adjacency with the neighbor, if any.

list ospf lsdb all This command displays all Link State advertisements in this router's LSDB.

Syntax

```
list ospf lsdb all
```

- **Default Area**—A 32-bit integer uniquely identifying the default area.
- **Type**—Version of Link State advertisement. They include:
 - **Router**—Router Link State advertisements.
 - **Network**—Network Link State advertisements.
 - **Sum(mary)-net(work)**—Routes to network outside the area but outside the OSPF routing domain.
 - **Sum(mary)-ASB**—Routes to Autonomous System Border routers.
 - **ASE**—Autonomous System External route advertisements.
- **Router ID**—32-bit number uniquely identifying the originating router in the autonomous system.
- **Sequence Number**—32-bit signed integer starting with the value '800000001'h or '7FFFFFFF'h used to detect old and duplicate link state advertisements. The space of sequence numbers is linearly ordered so the larger the sequence number, the more recent the advertisement.
- **Age**—Age of the Link State advertisement in seconds.
- **Checksum**—Checksum of the complete contents of the advertisement except for the age field, allowing for the incrementing of an advertisement's age without updating the checksum. Commonly known as the Fletcher checksum.

list ospf neighbor This command displays the state of all neighbors with which the local router has a relationship with over its local attached interfaces.

Syntax

```
list ospf neighbor
```

- **IP Address/IF Index**—IP address this neighbor uses as its IP source address or, on interfaces without addresses, the corresponding value of ifIndex in the Internet Standard MIB.
- **Router ID**—The router_id of a neighboring router in the OSPF domain.
- **Area**—Area to which this neighbor belongs.
- **Priority**—Ranking this neighbor has in the designated router election algorithm. The value 0 signifies the neighbor is not eligible to become the designated router on this particular network.
- **State**—Status of this neighbor. *Full* (for broadcast networks) or *PTP* (for WANs) indicates full adjacency has been established and the OSPF database has been synchronized. *ExStart* indicates that the process to establish

adjacency has been established, but full adjacency has not been established. A neighbor adjacency state of *TwoWay* is the expected state of two neighbor routers when neither is the designated router or backup designated router.

- **Event**—Sum of instances the router card/neighbor relationship has changed state or an error has occurred.
- **QLength**—Current length of the retransmission queue.
- **Status**—Dynamic status indicates that this neighbor was discovered using the Hello protocol.

list ospf receivepolicy This command displays all configured receive policies in OSPF.

Syntax

```
list ospf receivepolicy
```

- **Address/Mask**—The network address and mask describes the network match range.
- **Action**—Action for the specified route. Indicates whether to accept or ignore.
- **Metric**—Optional metric value associated with this route.
- **Type**—Optional type associated with this route (Type I or Type II).

Related Commands

[add ospf receivepolicy](#)

[delete ospf receivepolicy <network_address/ mask>](#)

[set ospf receivepolicy <network_address/ mask>](#)

[show ospf receivepolicy <network_address>](#)

list ospf sendpolicy This command displays all configured send policies in OSPF.

Syntax

```
list ospf sendpolicy
```

It lists the following information:

- **Source**
 - **ANY**
 - **OSPFEX**—NSSA translating type-7 to type-5
- **Address/Mask**—The network address and mask describes the network match range.

- **Action**—Action for the specified route. Indicates whether or not to advertise.

Related Commands

[add ospf sendpolicy](#)
[delete ospf sendpolicy](#)
[set ospf sendpolicy](#)
[show ospf sendpolicy](#)

set ospf area This command configures OSPF default area parameters.

Syntax

```
set ospf area <area_id>
    area_type [stub | transit]
```

Table 145 Set OSPF Command Parameters Descriptions

Parameter	Description
area_id	IP address of the OSPF area
area_type	Characteristic of the OSPF area. If <i>Stub</i> is configured, the area will not support importing of AS external link-state advertisements. <i>Transit</i> denotes the area can support importing AS external link-state advertisements. The default is Transit .

Related Commands

[delete ospf default_area](#)
[disable ospf area](#)
[enable ospf area](#)
[set ospf default_area_id](#)
[show ospf area <area_id> settings](#)

**set ospf
cryptographic_key**

This command configures a cryptographic key for the specified interface created with the `add ospf cryptographic_key` command. Each key is identified by the *interface* and associated *key id*. An interface may have multiple keys active at any one time. This enables smooth transition from one key to another. Each key has four time constants associated with it which can be expressed in terms of a time-of-day clock, or in terms of a router's local clock (e.g., number of seconds since last reboot).

Syntax

```
set ospf cryptographic_key <key_id>
    interface <ip_address or if_index>
    shared_key <password>
    start_accept <date.time>
    start_generate <date.time>
    stop_generate <date.time>
    stop_accept <date.time>
```

Table 146 Set OSPF Command Parameters Descriptions

Parameter	Description
key_id	Secret key used to create the message digest appended to the OSPF packet. Key Identifiers are unique per-interface. The range is 1-255.
interface	IP address or interface index of this OSPF interface.
shared_key	An alphanumeric string. The maximum size is 16 characters.
start_accept	The time the router card will start accepting packets that were created with the configured key. For smooth key transition, <i>Start Accept</i> should be less than <i>Start Generate</i> . The default is Current time and date.
start_generate	The time the router card will start using the configured key for packet generation. The default is <i>Start accept</i> time plus 10 minutes.
stop_generate	The time the router card will stop using the key for packet generation. If <i>stop generate</i> and <i>stop accept</i> are left unspecified, the key's lifetime is infinite. For smooth key transition, <i>stop generate</i> should be less than <i>stop accept</i> . This parameter may be set manually to a value of infinity. The default is infinity.
stop_accept	The time the router card will stop accepting packets that were created with the given key. If <i>stop generate</i> and <i>stop accept</i> are left unspecified, the key's lifetime is infinite. This parameter may be set manually to a value of infinity. The default is infinity.



When a new key replaces an old key, the Start Generate time for the new key must be less than or equal to the Stop Generate time of the old key

Date.time takes the form of DD-MMM-[YY]YY.HH:MM:SS. *The valid range of years is 1997 through 2036.* If only the date portion is specified, the time portion will be set to 0:0:0 of the day. If only the time portion is specified, the date portion will be set to the current date.



The parameters **stop_generate** and **stop_accept** will accept the value **infinity** in place of a *date.time* entry. If no value is entered, the default value for these parameters is **infinity**.

To achieve smooth key transition, `start_accept` should be less than `start_generate` and `stop_generate` should be less than `stop_accept`. If `stop_generate` and `stop_accept` are left unspecified, the key's lifetime is infinite. When a new key replaces an old key, the `start_generate` time for the new key must be less than or equal to the `stop_generate` time of the old key.

Related Commands

[add ospf cryptographic_key <key_id>](#)
[delete ospf cryptographic_key](#)
[list ospf cryptographic_key](#)
[show ospf cryptographic_key](#)

set ospf default_area_id

This command configures the default OSPF area where the router will be operating. The *area_id* is a 32-bit integer uniquely identifying an area. Area 0.0.0.0 is the OSPF Backbone. The default is **0.0.0.0**.

Syntax

```
set ospf default_area_id <area_id>
```

Related Commands

[delete ospf default_area](#)
[disable ospf area](#)
[enable ospf area](#)
[set ospf area](#)
[show ospf area <area_id> settings](#)

set ospf global

This command configures global OSPF parameters. Refer to the [show ospf global settings](#) to display configuration set by this command.

Syntax

```
set ospf global
  router_id <router_id>
  external_lsdb_limit <value>
  exit_overflow_interval <value>
  asbr [enable | disable]
  traps [enable | disable]
```



In order to change the OSPF global parameters you must first disable OSPF with the [disable ospf](#) command. When you have completed changing the OSPF global parameters use the [enable ospf](#) command to re-enable OSPF.



All OSPF routers must have the **external_lsdb_limit** parameter set to the same value. The number of link-state database entries is a function of the amount of memory in the router. The limit set should not allow more entries than can be accommodated by the router with the least amount of memory.

Table 147 Set OSPF Global Command Parameters Descriptions

Parameter	Description
router_id	A 32-bit integer uniquely identifying the router in the Autonomous System
external_lsdb_limit	Maximum number of non-default AS-external-LSA entries that can be stored in the link-state database. If the value is set to -1, there is no limit. If the value is set to 0 (zero), the router card will not allow any non-default AS-external-LSA entries to be stored in the link-state database. The range is -1 to 2147483647 . The default is -1 .
exit_overflow_interval	Number of seconds after entering OverflowState that a router tries to leave OverflowState. This allows the router to again originate non-default AS-external-LSAs. When set to 0, the router will not leave OverflowState until restarted. The range is 0 to 65535 . The default is 0 .
asbr	Administratively enables or disables configuration of the OSPF router to be an Autonomous System Boundary Router (ASBR). The default is disabled .
traps	Enables or disables traps. The default is enabled .

set ospf host

This command modifies the metric of a connected OSPF host. An OSPF *host* connection advertises within the OSPF routing domain only clients dialing into the router card who either do not use an aggregate IP address pool or are specially configured through Stub networks connected via a PPP link. See the [list ospf host](#) command for more information.

Syntax

```
set ospf host <IP address>
metric <1-65525>
```

Example

```
set ospf host 10.10.3.3 metric 10
```

set ospf interface This command configures parameters for the specified OSPF interface.

Syntax

```
set ospf interface <IP_address or IF_index>
  auth_key <password>
  auth_type [none | simple_password | cryptographic]
  hello_interval <1-65535>
  metric <1-16777215>
  retransmit_interval <1-3600>
  router_dead_interval <1-2147483647>
  router_priority <0-255>
  transit_delay <1-3600>
```



When you change the parameters for an OSPF interface the interface is automatically disabled then re-enabled which causes the new parameters to be put into effect. This is done automatically without user intervention.

Configure the following parameters.

Table 148 Set OSPF Interface Command Parameters Descriptions

Parameter	Description
auth_key	Authentication key. Only used when the interface's <i>auth-type</i> is set to <i>simple_password</i> . Maximum key length is up to 8 ASCII characters. Keys configured with less than 16 characters are left adjusted and zero filled to 8 characters. The default is zeros.
auth_type	Type of authentication used for the interface: <ul style="list-style-type: none"> ■ None—No password is used for the interface. ■ Simple_password—A password is used with the interface defined by the <i>auth_key</i>. ■ Cryptographic—Cryptographic Authentication is used with a cryptographic key defined on this OSPF interface. The default is None.
hello_interval	Period in seconds during which Hello packets are transmit over the interface. This value must be the same for all routers attached to a common network. The default is 10 seconds.
metric	Cost of sending a data packet out this interface. The range is 1 to 65535. The default is 1.
retransmit_interval	Number of seconds between link-state advertisement retransmissions, for adjacencies belonging to this interface. This value is also used when retransmitting database description and link-state request packets. The default is 5 seconds.

Table 148 Set OSPF Interface Command Parameters Descriptions

Parameter	Description
router_dead_interval	Number of seconds that a router's Hello packets have not been seen before its neighbors declare the router down. This value should be some multiple of the Hello interval. The default is 40 seconds. Note: This value must be the same for all routers attached to a common network.
router_priority	Priority of this interface to be used in designated router election. Designated router election is only applicable on multi-access networks. The higher the router_priority, the more likely the router will win in the designated router election for the network. A priority of zero indicates that the router is not eligible to participate in the designated router election process. In the event that two routers are tied in router_priority, the RouterID will be used as the tie breaker. The default is 5.
transit_delay	Estimated interval, in seconds, to transmit a link-state update packet over the specified interface. The default is 1 second.

Related Commands[disable ospf interface](#)[enable ospf interface](#)[show ospf interface <IP address or IF index> settings](#)**set ospf receivepolicy
<network_address/
mask>**

This command edits an OSPF import policy that can filter ASEs from the routing table. Also use this command to affect how ASEs are accepted into the routing table.

Syntax

```
set ospf receivepolicy <network_address/ mask>
    action [accept | ignore]
    routing_preference [pref0 | pref1 | pref2 | pref3]
```



An OSPF receive policy only affects an ASE when it is received. Once an ASE is in the LSDB (Link State Database) changing or adding a receive policy has no effect on the ASE.

When the action for the receivepolicy is set to accept, the routing_preference parameter is used to separate routes into groups that lead to the same destination. These groups are based on the protocol that generated the route. Choose the appropriate parameter (pref0, pref1, pref2, or pref3) depending on the preferred route. A lower preference value indicates a better route, i.e. pref0 has a lower preference than pref1, etc. If two routes have the same routing preference, then the route with the lower cost metric is used. It is important to remember that although a route assigned pref3 appears in the routing table, the route is never used to determine how to forward a packet. Essentially, a pref3 route is not used to forward packets.



Setting the `routing_preference` parameter to a value of `pref3` is equivalent to setting the `action` parameter to a value of `ignore`.
 If the `action` parameter is set to a value of `ignore`, the `routing_preference` value has no effect. Changing the `action` parameter to a value of `accept` at a later time puts the stored `routing_preference` value into effect.

Typically, both static routes and routes generated by RIP get assigned a routing preference equivalent to `pref 1` (or OSPF external type 1 routes). Conversely, OSPF internal routes are preferred over RIP-generated or static routes.

Table 149 Set OSPF Receiving Command Parameters Descriptions

Parameter	Description
<code>network_address/mask</code>	The network address and mask describes the network match range. An external route of an ASE whose most significant bits match the portion of the policy's network address defined by the mask will be received or not (depending on the action specified in the routing table). The mask defines the number of consecutive bits, starting from the most significant bit to the least significant bit, that must match. The mask may be specified as a value from 8 to 32, or alternatively be entered in the format of an IP address class (A, B or C). No mask entry will result in a default mask being generated that matches the class of the specified network address.
<code>action</code>	Configures whether to accept or ignore the specified route.
<code>routing_preference</code>	When the action for this receivepolicy is set to <code>accept</code> , you can specify the preferred route as one of the following: <ul style="list-style-type: none"> 0—Selects a routing preference equivalent to OSPF internal routes. 1—Selects a routing preference equivalent to OSPF external type 1 routes. 2—Selects a routing preference equivalent to OSPF external type 2 routes. 3—Signifies that the route is not used.

Related Commands

[`add ospf receivepolicy`](#)

[`delete ospf receivepolicy <network_address/ mask>`](#)

[`list ospf receivepolicy`](#)

[`show ospf receivepolicy <network_address>`](#)

set ospf sendpolicy This command edits a send policy (route leak) for the given destination.

Syntax

```
set ospf sendpolicy <network_address/mask>
  action [advertise | do_not_advertise]
  metric <0 to 16777215>
  metric_type [type_i | typeii]
  source [local | rip | remote]
  tag <0 to 2147483647>
```



When a send policy is added or modified the routing table is fully scanned automatically for a route and send policy match. This requires no user intervention. If a match is found and an ASE does not exist a new ASE is generated. If a match is found and an ASE exists and parameters have changed in its associated send policy the ASE is re-originated with the modified information.

Configure the following parameters.

Table 150 Set OSPF SendPolicy Command Parameters Descriptions

Parameter	Description
network_address/mask	The network address and mask describes the network match range.
action	Configures whether to redistribute (advertise) or block (not advertise) the specified route.
metric	Optional. Selects the metric value to be placed in an ASE. Setting this to 0 reads the metric value associated with a route contained in the routing table. Any other value (1-16777215) is used as the metric value that is placed in an ASE. The default is 0 . The range is 0-16777215 .
metric_type	Optional. Configures the type of cost associated with external routes. Type 1 metrics represent the total cost of all steps (internal and external) between a source and a destination. Type 2 metrics represent only the cost of the external path to the destination.
source	Route source including local and remote static routes, routes learned via RIP.
tag	Optional tag. Values range from 0 to 2147483647 .

Related Commands

[add ospf sendpolicy](#)

[delete ospf sendpolicy](#)

[list ospf sendpolicy](#)

[show ospf sendpolicy](#)

show ospf This command displays OSPF default area and send policy information.

Syntax

```
show ospf
    default_area_id
    sendpolicy <IP address> source [local | remote | rip]
```

Table 151 Show OSPF Command Parameters Descriptions

Parameter	Description
default_area_id	Displays the default 32-bit integer uniquely identifying the OSPF area.
sendpolicy source	Displays the specified OSPF send policy route source including local and remote static routes, routes learned via RIP.

show ospf area <area_id> settings

This command displays the specified OSPF area configuration. It lists the following information:

- **Area ID**—IP address of the OSPF area
- **Area Status**—Displays the area status. Enabled denotes the area is in an active state. Disabled denotes the area is in an inactive state; either the area was administratively disabled or OSPF was globally disabled.
- **Area Type**—Indicates if the area is configured as a *Stub* or *Transit* area.

Syntax

```
show ospf area <area_id> settings
```

Related Commands

[delete ospf default_area](#)

[disable ospf area](#)

[enable ospf area](#)

[set ospf area](#)

[set ospf default_area_id](#)

**show ospf
cryptographic_key**

This command displays the configuration of the OSPF encrypted password.

Syntax

```
show ospf cryptographic_key <number>
    interface <ip_address>
```



*If no cryptographic key has been configured for an OSPF interface, the default Cryptographic key with key_id = 0 will be used for authentication. This default key can not be deleted and cannot be displayed by the **list** or **show** commands. The lifetime of the default key is infinite.*

The command lists the following information:

- **Interface IP Address**—IP address of the OSPF interface with which this cryptographic key is associated.
- **Address Less Ifindex**—Addressless interface Index number of the OSPF interface with which this cryptographic key is associated.
- **Key ID**—Key identifier of a secret key used to create the message digest appended to the OSPF packet. Key Identifiers are unique per-interface.
- **Status**—Operational status of this key. When the key status is *Active*, this means that the router has either authenticated an OSPF packet using this key for one of its neighbors on this OSPF interface, or the router has started generating a message digest for sending OSPF packets out of this OSPF interface. It is possible to have two keys that are in *Active* status when the router is in the key transition phase on the interface. One key is used when authenticating received OSPF packets and the other is used when the router begins to send OSPF packets. Otherwise, the key status is *NotInService*.
- **Start Accept**—The time (*dd-mmm-yy.hh:mm:ss*) the router card starts accepting packets that were created with the configured key. For smooth key transition, Start Accept should be less than Start Generate. The default is Current time and date.
- **Start Generate**—The time (*dd-mmm-yy.hh:mm:ss*) the router card starts using the configured key for packet generation. For smooth key transition, stop generate should be less than stop accept. The default is the Start generate time plus 10 minutes.
- **Stop Generate**—The time (*dd-mmm-yy.hh:mm:ss*) the router card stops using the key for packet generation. If stop generate and stop accept are left unspecified, the key's lifetime is infinite. The default is Stop generate and stop accept = infinity.
- **Stop Accept**—The time (*dd-mmm-yy.hh:mm:ss*) the router card stops accepting packets that were created with the given key. If stop generate and stop accept are left unspecified, the key's lifetime is infinite.

Related Commands

[add ospf cryptographic_key <key_id>](#)

[delete ospf cryptographic_key](#)

[list ospf cryptographic_key](#)

[set ospf cryptographic_key](#)

show ospf global settings

This command displays global OSPF configuration.

Syntax

```
show ospf global settings
```

- **Router ID**—IP address of the OSPF router.
- **Administrative Status**—Working status of the OSPF router.
Enabled—OSPF is in an active state or, **Disabled**—OSPF is in an inactive state.
- **OSPF Version Number**—Version of OSPF that is supported.
- **Area Border Router Status**—The Area Border Router status of the router.
Enabled denotes the router is functioning as an ABR. Disabled states the router is not functioning as an ABR. Only supported value is **Disabled**.
- **AS Boundary Router Status**—The AS Boundary Router status of the router. **Enabled** denotes the router is functioning as an ASBR. Disabled states the router is not functioning as an ASBR.
- **External LSDB Limit**—The maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database. If the value is -1, there is no limit.
- **Multicast Extensions Support**—Indicates if OSPF multicast extensions are supported. This field is always **Off**.
- **Exit Overflow Interval**—Number of seconds after entering OverflowState that the router will attempt to leave OverflowState.
- **On-Demand Extensions**—Indicates if OSPF on-demand extensions are supported. This field is always Off
- **SNMP Trap**—Indicates if SNMP traps are enabled or disabled.

Related Commands

[set ospf global](#)

**show ospf interface <IP
address or IF index>
settings**

This command displays the configuration of the specified OSPF interface.

Syntax

```
show ospf interface <IP address or IF index> settings
```

- **Interface IP Address**—IP address of the specified OSPF interface.
- **AddressLess IfIndex**—Used to ease the instancing of addressed and addressless interfaces. This variable takes the value **0** on interfaces with *IP address*, or the corresponding value of **ifIndex** for interfaces having no IP addresses.
- **Area ID**—32-bit integer uniquely identifying the area to which the specified interface connects.
- **Interface Type**—The specified OSPF interface type.
 - **BC**—Broadcast LANS, such as Ethernet and ATM.
 - **PTOP**—Links that are point-to-point types, such as PPP and Frame Relay connections.



For the purposes of configuring OSPF, CommWork's implementation of ATM in the router card treats ATM as a broadcast network. In this implementation, the router card simulates a broadcast network over ATM by sending data traffic over all configured ATM PVCs.

- **Administrative Status**—The specified OSPF interface's admin status.
- **Router Priority**—Priority of the specified OSPF interface.
- **Transit Delay**—Transit delay period in seconds.
- **Retransmit Interval**—Retransmit period in seconds.
- **Hello Interval**—The hello interval in seconds.
- **Router Dead Interval**—Period, in seconds, during which if the router does not see a hello from its neighbor, before the router flags that neighboring router as dead.
- **OSPF Interface State**—Indicates state of the specified interface. States supported are as follows:
 - **Down**—Not operational.
 - **Loopback**—Diagnostic.
 - **Waiting**—Waiting to determine its role (Designated Router, Backup Designated Router or Other).
 - **PointToPoint**—Point-to-Point interface.
 - **DsgRtr**—the Designated Router.
 - **BackupDsgRtr**—the Backup Designated Router.
 - **otherDsgRtr**—*not* the Designated Router nor Backup Designated Router.
- **Designated Router Address**—IP address of the Designated Router.

- **Backup Designated Router Address**—IP address of the Backup Designated Route.
- **Authentication Type**—Specifies authentication level supported.
- **OSPF Interface Demand**—*Off* indicates on-demand extensions are not supported on the specified interface.
- **Metric Value**—The interface metric.

Related Commands

[disable ospf interface](#)

[enable ospf interface](#)

[set ospf interface](#)

**show ospf interface <IP
address or IF index>
counters**

This command displays counters for the specified OSPF interface.

Syntax

```
show ospf interface <IP address or IF index> counters
```

- **Interface IP Address**—IP address of the specified OSPF interface.
- **AddressLess IfIndex**—Used to ease the instancing of addressed and addressless interfaces. This variable takes the value **0** on interfaces with *IP address*, or the corresponding value of **ifIndex** for interfaces having no IP addresses.
- **Area ID**—32-bit integer uniquely identifying the area to which the specified interface connects.
- **Events Count**—Number of times the specified OSPF interface has changed its state or an error has occurred.

Related Commands

[disable ospf interface](#)

[enable ospf interface](#)

[set ospf interface](#)

show ospf lsdb This command displays Link-state Database which consists of all Link State Advertisements that originated from the local router and other routers in the OSPF routing domain.

Syntax

```
show ospf lsdb
    default_area <ip_address>
    router_id <ip_address>
    type <router, network, sum-network, sum-asb, ase>
```

- **default_area**—A 32-bit integer uniquely identifying the default area.
- **router_id**—The ip address of the ASBR.
- **type**—Version of Link State advertisement. They include:
 - **router**—Router Link State advertisements.
 - **network**—Network Link State advertisement.
 - **sum-net**—(Summary-network) Routes to network outside the area but outside the OSPF routing domain.
 - **sum-ASB**—(Summary-ASB) Routes to Autonomous System Border routers.
 - **ase**—Autonomous System External route advertisements.

show ospf receivepolicy <network_address> This command displays the configuration of the specified OSPF receive policy.

Syntax

```
show ospf receivepolicy <network_address>
```

Related Commands

```
add ospf receivepolicy
set ospf receivepolicy <network\_address/ mask>
delete ospf receivepolicy <network\_address/ mask>
list ospf receivepolicy
```

show ospf sendpolicy This command displays the configuration of the specified OSPF send (route leak) policy.

Syntax

```
show ospf sendpolicy <network_address/mask>
```

Related Commands

[add ospf sendpolicy](#)

[delete ospf sendpolicy](#)

[list ospf sendpolicy](#)

[set ospf sendpolicy](#)

PPP

This section covers commands that configure Point to Point Protocol functions using the CLI.

add datalink ppp user <username> This command add a PPP data link layer.

Syntax

```
add datalink ppp user <username>
    enabled [no | yes]
    interface <interface_name>
```

Table 152 Add Datalink PPP User Command Parameters Descriptions

Parameter	Description
<user_name>	A valid user name. The limit is 32 ASCII characters.
enabled	Enable or disable the user. Values is enabled or disabled .
interface	The name of a valid interface. The limit is 32 ASCII characters .

delete datalink ppp interface This command removes the PPP data link layer defined on top of the physical WAN interface. You can list currently defined PPP datalink enabled interfaces using the [list ppp](#) command.

Syntax

```
delete datalink ppp interface <interface_name>
```

Related Commands

[list ppp](#)

disable ilmi This command disables Interim Link Management Interface (ILMI) address registration supporting network management functions between users and the network.

Syntax

```
disable ilmi [atmaal:1 | atmaal:2]
```

Example

Related Commands

[enable ilmi](#)

For more configuration information, see the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

disable ppp acct_for_abnormal_disc This command disables the sending of an Accounting Stop record when a call is abnormally disconnected before a Start Record is sent.

Syntax

```
disable ppp acct_for_abnormal_disc
```

Example

```
disable ppp acct_for_abnormal_disc
```

Related Commands

[enable ppp acct_for_abnormal_disc](#)

[show ppp settings](#)

disable ppp address_field_compression This command disables PPP address field compression. The default is enabled.

Syntax

```
disable ppp address_field_compression
```

Example

```
disable ppp address_field_compression
```

Related Commands

[enable ppp address_field_compression](#)

[show ppp settings](#)

disable ppp bacp_bap This command disables the router card's BACP/BAP feature. This feature is disabled by default.

Syntax

```
disable ppp bacp_bap
```

Example

```
disable ppp bacp_bap
```

Related Commands

[enable ppp bacp_bap](#)

[show ppp settings](#)

disable ppp multilink_ppp This command disables negotiation of multilink parameters for PPP calls.

Syntax

```
disable ppp multilink_ppp
```

Example

```
disable ppp multilink_ppp
```

Related Commands

[enable ppp multilink_ppp](#)

[show ppp settings](#)

disable ppp offloading This command disables any PPP attempt to offload framing to modem cards.

Syntax

```
disable ppp offloading
```

Example

```
disable ppp offloading
```

Related Commands

[enable ppp offloading](#)

[show ppp settings](#)

**disable ppp
protocol_field_
compression**

This command disables PPP protocol field compression. The default is enabled.

Syntax

```
disable ppp protocol_field_compression
```

Example

```
disable ppp protocol_field_compression
```

Related Commands

[enable ppp protocol_field_compression](#)

[show ppp settings](#)

**disable ppp
receive_accm**

This command disables strict checking of receive side ACCM mapping for incoming PPP data packets. It checks whether all the control characters which need to be mapped are mapped in all data packets.

Syntax

```
disable ppp receive_accm
```

Example

```
disable ppp receive_accm
```

**disable datalink ppp
interface**

This command disables the administrative state of the PPP DLL created on top of the physical WAN interface. Use the [list ppp](#) command to list currently defined PPP datalink enabled interfaces.

Syntax

```
disable datalink ppp interface <interface_name>
```

Example

```
disable datalink ppp interface eth1
```

enable atm1483 pvc

This command enables a PVC you created for RFC-1483 compliant networks with the `add atm1483 pvc` command. For more configuration information, see *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*

Syntax

```
enable atm1483 pvc <name>
```

Example

```
enable atm1483 pvc conn3
```

Related Commands

[add atm1483 pvc](#)
[delete atm1483 pvc](#)
[disable atm1483 pvc](#)
[list atm1483 pvcs](#)
[show atm1483 pvc <name> settings](#)

enable atm1577 pvc This command enables a PVC you created for RFC-1577 compliant networks with the `add atm1577 pvc` command. For more configuration information, see *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Syntax

```
enable atm1577 pvc <name>
```

Related Commands

[add atm1577 pvc](#)
[delete atm1577 pvc](#)
[disable atm1577 pvc](#)
[list atm1577 pvcs](#)
[show atm1577 pvc <name> settings](#)

enable atmsig This command enables the User-Network Interface (UNI) signaling configuration on the specified ATM network. For more configuration information, see *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Syntax

```
enable atmsig
```

Related Commands

[disable atmsig](#)

enable datalink ppp interface

This command enables PPP as the datalink layer protocol to run on the specified interface. You must have previously run `add datalink ppp` in order for this command to work. You can list currently defined PPP datalink enabled interfaces using [list ppp](#).

Syntax

```
enable datalink ppp interface <interface_name>
```

Related Commands

[list ppp](#)

enable ilmi

This command enables Interim Link Management Interface (ILMI) address registration which supports network management functions between the user-side and network-side of the ATM UNI (User-Network Interface) interface. User-side configuration concerns customer premises equipment while network-side configuration concerns the network switch. For more configuration information, see the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Syntax

```
enable ilmi [atmaal:1 | atmaal:2]
```

Related Commands

[disable ilmi](#)

enable ppp acct_for_abnormal_disc

This command enables the sending of an Accounting Stop record when a call is abnormally disconnected before a Start Record is sent.

Syntax

```
enable ppp acct_for_abnormal_disc
```

Related Commands

[disable ppp acct_for_abnormal_disc](#)

[show ppp settings](#)

enable ppp address_field_compression

This command enables PPP address field compression. The default is enabled.

Syntax

```
enable ppp address_field_compression
```

Related Commands

[disable ppp address_field_compression](#)

[show ppp settings](#)

enable ppp bacp_bap This command enables the router card's BACP/BAP feature. This feature is disabled by default.

Syntax

```
enable ppp bacp_bap
```

Related Commands

[disable ppp bacp_bap](#)

[show ppp settings](#)

enable ppp multilink_ppp This command enables negotiation of multilink parameters for PPP calls.

Syntax

```
enable ppp multilink_ppp
```

Related Commands

[disable ppp multilink_ppp](#)

[show ppp settings](#)

enable ppp offloading This command enables PPP attempts to offload PPP framing to modem cards. The default is enabled.

Syntax

```
enable ppp offloading
```

Related Commands

[disable ppp offloading](#)

[show ppp settings](#)

enable ppp receive_accm This command enables strict checking of receive side ACCM mapping for incoming PPP data packets. It checks whether all the control characters which need to be mapped are mapped in all data packets.

Syntax

```
enable ppp receive_accm
```

Related Commands

[disable ppp receive_accm](#)

**enable ppp
protocol_field_
compression**

This command enables PPP protocol field compression. The default is **enabled**.

Syntax

```
enable ppp protocol_field_compression
```

Example

```
enable ppp protocol_field_compression
```

Related Commands

[disable ppp protocol_field_compression](#)

[show ppp settings](#)

**enable ppp
radius_challenge_
with_pap**

This command enables PPP reauthentication using PAP.

Syntax

```
enable ppp radius_challenge_with_pap
```

Example

```
enable ppp radius_challenge_with_pap
```

Related Commands

[disable ppp radius_challenge_with_pap](#)

**disable ppp
radius_challenge_with_
pap**

This command disables PPP reauthentication using PAP.

Syntax

```
disable ppp radius_challenge_with_pap
```

Example

```
disable ppp radius_challenge_with_pap
```

Related Commands

[enable ppp radius_challenge_with_pap](#)

monitor ppp

This command allows monitoring of realtime PPP activity. For best results, CommWorks recommends that you use this program via TELNET. The router card offers the following three methods for you to use to evaluate PPP events:

- The **tap** command to check raw data.
- The **set facility** and **show events** commands to record data via syslogs.
- The **monitor ppp** command to employ protocol decoding.

Before using the **monitor PPP** command, you must first issue a **show events** command as a managed user who is dialed in or connected across the network with telnet. **Monitor ppp** is limited to checking PPP data streams. It can neither

monitor network traffic nor capture data and direct it to a SYSLOG host or your console as with the **tap** commands.

The command performs the following monitoring options:

- **(C) Monitor PPP call events**—Displays internal PPP states as they change for each interface. Most of these events are displayed as events if the proper logging level is set for PPP. This is the only monitoring option that displays the action of more than one PPP session.
- **(I) Monitor a specific interface**—Displays all PPP packets transmitted and received on the specified interface. If a session already is occurring on the specified interface, monitoring will begin immediately. If not, monitoring will begin with the next session on that interface. If one session stops and starts, monitoring will continue.
- **(N) Monitor the next session that starts up**—Displays results for next PPP session created. This option is useful if a user is having difficulty connecting and it's unclear which interface the user will connect on because of his inclusion in a hunt group. As soon as the next incoming or outgoing PPP call is established, monitoring will begin. There is no differentiation on the next session—the user selects to monitor the next session and will see the next session displayed regardless of interface or user name employed.



Only one monitor may be used for Next Session at any one time.

- **(U) Monitor a specific user**—Displays any PPP sessions currently active for the specified user. As any new session begins for the user, monitoring will also begin. This is the best method to display data from a multi-link session.



Since the PPP session does not have a user associated with it until authentication occurs, this method of monitoring will not permit tracing of the authentication negotiation.

- **(T) Monitor a specific calling number**—Displays any PPP sessions currently active for the specified number.
- **(X) Exit the monitor**—Exits the program.

Monitoring Stop/Start

When monitoring begins, a variety of information is displayed with some options available to you. When I is selected, as soon as data entry is validated the program displays messages that the decode tracing has started and proceeds to trace the interface.

All output is paused until you press **ENTER**. If you press **ESC**, monitoring stops and the main menu is displayed again.

Once you press **ESC**, you have the option of pressing **ENTER** again to continue monitoring or **ESC** once again to terminate monitoring and return to the main menu.



All PPP packets sent or received while the monitor is “paused” are lost and not saved waiting for the program to resume. Also, if a call is dropped at any time, you must return to the monitor and start again.

Idle Timer

If you pressed **U**, while monitoring is active and as long as no data is displayed, the program displays an idle message verifying that it is active. When monitoring data is displayed, the idle message does not appear.

Decode and Hexadecimal Display

Interface, User, and Next Session monitoring display two types of data, *decode* and *hexadecimal*. *Decode*, the default, displays packets without decompression in a textual, decoded output. *Hexadecimal* displays packets with decompression in hexadecimal and any ASCII equivalent as soon as they are received or just before transmission. Both modes can be switched on the fly. Decode displays only the initial 15 to 20 characters of the packet.

To switch from decode mode to hexadecimal mode, type **H** or **X** (not case-sensitive). To switch back to decode mode, type **D**.



There may be a lag due to delayed output to the screen.

```
show ppp on interface <slot:x/mod:y>
```

```
show ppp on interface settings
```

Displays PPP settings on the specified WAN interface when interface is active, listing the following information:

Settings For PPP Bundle 1

- **Operational Status**—*Opened or Not Opened*.
- **Number Active Links**—Number of links active on this PPP bundle.
- **User Profile**—User whose parameters were used in creating links.
- **Local MMRU**—MRU the remote entity uses when sending packets to local PPP entity. The default is **1514**.
- **Remote MMRU**—MRU the local entity uses when sending packets to remote PPP entity. The default is **1514**.
- **Local Endpoint Class**—Type of address used as the identifier—**IEEE MAC address**.
- **Local Endpoint Length**—Maximum length of the local Endpoint Discriminator address. The default is **6**.
- **Local Endpoint ID**—*MAC address* of local Endpoint Discriminator.
- **Remote Endpoint Class**—Value of remote Endpoint Discriminator Class, which indicates the type of address being used as the identifier.

- **Remote Endpoint Length**—Maximum length of remote Endpoint Discriminator address.
- **Remote Endpoint ID**—*IP address* of remote Endpoint Discriminator.

Settings For PPP Bundle 1 Compression

- **Operational Status**—*Opened or Not Opened*.
- **Compression Protocol**—Protocol used by the local PPP entity when it compresses the local PPP entity to the remote PPP entity. The default is **VJ-TCP**.

Settings for PPP Link

- **Operational Status**—*Opened or Not Opened*.
- **Interface Index**—Index number of the interface used.
- **Local MRU**—The MRU the remote entity uses when sending packets to local PPP entity. The default is **1514**.
- **Remote MRU**—The MRU the local entity uses when sending packets to remote PPP entity. The default is **1514**.
- **Local to Peer ACC Map**—Value of the ACC Map used for sending packets from the local PPP entity to the remote PPP entity.
- **Peer to Local ACC Map**—ACC Map used by the remote PPP entity when transmitting packets to the local PPP entity.
- **Local To Remote Protocol Compression**—Indicates whether the local PPP entity will use Protocol Compression when transmitting packets to the remote PPP entity. The default is **enabled**.
- **Remote To Local Protocol Compression**—Indicates whether the remote PPP entity will use Protocol Compression when transmitting packets to the local PPP entity. The default is **enabled**.
- **Local To Remote ACC Compression**—Indicates whether the local PPP entity will use address and Control Compression when transmitting packets to the remote PPP entity. The default is **enabled**.
- **Remote To Local ACC Compression**—Indicates whether the remote PPP entity will use address and Control Compression when transmitting packets to the local PPP entity. The default is **enabled**.

Settings For PPP Link—Authentication

- **Operational Status**—*Opened or Not Opened*
- **Local To Remote Compression Protocol**—Protocol used by the local PPP entity when it compressed the remote PPP entity. The default is **CHAPMD5**.
- **Remote To Local Compression Protocol**—Protocol used by the remote PPP entity when it compressed the local PPP entity.

show ppp settings This command displays global settings for PPP. Use the `receive_authentication` parameter of the [set ppp](#) command to modify DIAL-IN users authentication. Use [set system](#) to modify the system transmit authentication name.

Syntax

```
show ppp settings
```

- **DIAL-IN Users Authenticate PAP or CHAP**—Indicates whether PPP requires dial-in users to authenticate strictly via *PAP, CHAP, ANY, EAP-MD5; with ANY, NONE, or ENCRYPTED-ANY (CHAP, EAP-MD-5, MS-CHAP) or RADIUS-EAP-PROXY*. The default is *None*.
- **System Transmit Authentication Name**—Remote account keyword used by PPP at the datalink layer for WAN connections.
- **PPP offloading**—Indicates, when enabled, that PPP framing can be off-loaded to the modem card, if modem card is capable of doing it. The default is **enabled**.
- **CCP attempted for call types**—Indicates the types of call for which the Compression Control Protocol will be enabled in the router card PPP module. Possible values are *all, none, digital, compressed analog* and *uncompressed analog*. Default value: **digital** and **uncompressed analog**.
- **Primary NBNS Server address**—IP address for the primary NetBIOS Name Server (NBNS) server. In the absence of a user-specific NBNS address, this will be sent in IPCP negotiation.
- **Secondary NBMS Server address**—IP address for the secondary NetBIOS Name Server (NBNS) server. In the absence of a user-specific NBNS address, this will be sent in IPCP negotiation.
- **DNS Configuration Usage**—Indicates, when enabled, that PPP will take DNS addresses from the router card's DNS table in the absence of user-configured DNS addresses. Choices: *SYSTEM, PPP* or *NONE*.
- **Primary PPP DNS Server address**—Globally configured PPP DNS primary server IP address, used if user-configured DNS addresses are not available, for IPCP (IP Control Protocol) negotiation.
- **Secondary PPP DNS Server address**—Globally configured PPP DNS secondary server IP address, used if user-configured DNS addresses are not available, for IPCP (IP Control Protocol) negotiation.
- **Session Start Message**—Displays string you specified to indicate the beginning of a PPP session.
- **Send Accounting for PPP Abnormal Disc**—Sending of an Accounting Stop record when a call is abnormally disconnected before a Start Record is sent.
- **PPP Address Field Compression**—Displays the state of PPP address field compression, enabled or disabled.
- **PPP Protocol Field Compression**—Displays the state of PPP protocol field compression, enabled or disabled.
- **PPP Multilink PPP**—Displays the state of the MLPPP (Multilink PPP) support.

- **PPP BACP and BAP**—Displays the state of BACP/BAP support.
- **PPP Bap Hunt Group Phone Number**—The phone number set for the Band Allocation Protocol (BAP) hunt group.

enable ppp send_edo This command enables sending the PPP EDO option in the LCP configure request.

Syntax

```
enable ppp send_edo
```

Example

```
enable ppp send_edo
```

Related Commands

[disable ppp send_edo](#)

disable ppp send_edo This command disables sending the PPP EDO option in the LCP configure request.

Syntax

```
disable ppp send_edo
```

Example

```
disable ppp send_edo
```

Related Commands

[enable ppp send_edo](#)

PPPoE Commands

This section covers commands that configure PPP over Ethernet using the CLI.

add pppoe service_name

During the discover stage of the PPPoE protocol, the PPPoE client may request a connection with the router card indicating the service name that it requires. The service name is typically the name of the ISP or any QOS parameters.

Presently the service names are just strings with no QOS significance attached. The client may send a service name as a NULL string indicating that any service is acceptable in which case no service names need to be configured in the router card. If the client request contains a non-null service name in the request, then the same name has to be configured in the router card.

Syntax

```
add pppoe service_name <name>
```

Related Commands

For more information refer to *RFC 2516*.

delete pppoe service_name This command removes the designated PPPoE service name.

Syntax

```
delete pppoe service_name <name>
```

Related Commands

[add pppoe service_name](#)

disable pppoe on interface This command disables the specified interface from sending or receiving frames carrying the new ether-type defined by the PPPoE protocol.

Syntax

```
disable pppoe on interface <interface_name>
```

Related Commands

[enable pppoe on interface](#)

enable pppoe on interface This command enables the specified interface to send and receive frames carrying the new ether-type defined by the PPPoE protocol.

Syntax

```
enable pppoe on interface <interface_name>
```

Related Commands

[disable pppoe on interface](#)

show pppoe This command displays PPPoE statistics.

Syntax

```
show pppoe
```

- **PPPoE Session ID**—The session identifier for this session.
- **PeerAddress**—The MAC address for the session peer.

Example

```
show pppoe
```

Related Commands

[list pppoe](#)

list pppoe This command shows information about PPPoE interfaces, service names, and sessions.

Syntax

```
list pppoe
    bindings
    service_names
    sessions
```

Table 153 List PPPOE Command Parameters Descriptions

Parameter	Description
bindings	This lists all the interfaces where PPPoE has been enabled and the status.
service_names	The service name is typically the name of the ISP or any QOS parameters. Presently the service names are just strings with no QOS significance attached. The client may send a service name as a NULL string indicating that any service is acceptable in which case no service names need to be configured in the router card. If the client request contains a non-null service name in the request, then the same name has to be configured in the router card.
sessions	This command lists all of the existing PPPoE sessions and their peer addresses in the concentrator.

Example

```
list pppoe
```

Related Commands

[add pppoe service_name](#)

list virtual connections This command lists all of the PPPoE connections coming into the router card as well as tunneled connections such as PPTP, L2TP etc. This command exists in addition to the list tunnel connections command which only displays the virtual connections made by PPTP, L2TP etc.

Syntax

```
list virtual connections
```

Example

```
list virtual connections
```

Related Commands

[list pppoe](#)

set pppoe This command sets parameters for PPPoE sessions.

Syntax

```
set pppoe
```

```
max_sessions <number>
max_sessions_per_host <number>
```

Table 154 Set PPPOE Command Parameters Descriptions

Parameter	Description
max_sessions	The maximum number of PPPoE connections that may be initiated concurrently to the router card by all hosts combined.
max_sessions_per_host	The maximum number of PPPoE connections that may be initiated concurrently by a single host to the router card. This helps to limit the Denial of Service attacks on the router card.

Example

```
set pppoe
```

Related Commands

[list pppoe](#)

Tunneling

list all sessions vpn This command displays all active tunnel sessions for the specified domain name. While not displayed by this command, the domain name appears in the **list all tunnels** output.

Syntax

```
list all sessions vpn <domain name>
```

Related Commands

[list all tunnels](#)

list all tunnels This command displays settings and statistics for all active tunnels on the system. Information for both LAC and LNS devices is displayed. This command is useful for Internet Service Providers offering domain-based tunnel services.

Syntax

```
list all tunnels
```

Related Commands

[list all sessions vpn](#)

list tunnel connections This command displays tunnel information for all tunnels configured with the [set tunnel user](#) command.

Syntax

```
list tunnel connections
```

Example

```
list tunnel connections
```

Related Commands

[set tunnel user](#)

set global_call_type This command configures all calls as PPTP or L2TP calls, for use in systems where only PPTP or L2TP calls are made. This default can be disabled with the *none* value. This command effects immediate VPN tunnelling without authentication to limit network overhead.

Syntax

```
set global_call_type [pptp | l2tp | none]
```

Example

```
set global_call_type l2tp
```

show global_call_type settings This command displays configuration for a router card placing L2TP or PPTP (or NONE) calls only. The default is None.

Syntax

```
show global_call_type settings
```

Example

```
show global_call_type settings
```

Related Commands

[set global call type](#)

show pptp tunnel This command displays statistics of the specified PPTP tunnel.

Syntax

```
show pptp tunnel <0 to 65535>
```

- **Local control tunnel ID**—Identifier of the specified local control tunnel
- **Peer control tunnel ID**—Identifier of the specified remote control tunnel
- **Control tunnel state**—Current status of the specified control tunnel
- **Local init connection**—Indicates whether tunnel was established locally or not
- **IP address**—Remote peer's IP address
- **Local receive packet window**—Size of local send window
- **Remote receive packet window**—Size of remote receive window

- **Control tunnel receive packets**—Sum of control packets received on the control tunnel
- **Control tunnel receive packets with data**—Sum of control packets received with data
- **Control tunnel receive packets without data**—Sum of zero length packets received
- **Processed control tunnel receive packets**—Sum of receive packets that were processed
- **In sequence control tunnel receive packets**—Sum of packets received in sequence
- **Out of sequence control tunnel receive packets**—Sum of packets received out of sequence
- **In order control tunnel receive packets**—Sum of packets received in order
- **Out of order control tunnel receive packets**—Sum of packets received out of order
- **Flow discarded control tunnel receive packets**—Sum of received packets discarded due to flow control
- **Out of order discarded control channel receive packets**—Sum of received packets discarded due to ordering
- **Control tunnel send packets**—Sum of packets transmitted
- **Control tunnel send packets with data**—Sum of packets transmitted with data
- **Control tunnel send packets without data**—Sum of zero length packets transmitted
- **Control tunnel flow control timeouts**—Sum of timeouts caused by flow control
- **Control tunnel flow control on**—Status of local flow control: **enabled** or **disabled**
- **Local control tunnel flow control enables**—Sum of local flow control enables for the control session
- **Remote control tunnel flow control on**—Status of remote flow control: **enabled** or **disabled**
- **Remote control tunnel flow control enables**—Sum of remote flow control enables for the control session
- **Control tunnel reassembly timeouts**—Sum of reassembly timeouts
- **Remote host name**—Host name of the PPTP peer

Example

```
show pptp tunnel 10
```

Related Commands

[list pptp tunnel <number> sessions](#)

[list pptp tunnels](#)

[show pptp tunnel <number> session <number>](#)

**show pptp tunnel
<number> session
<number>**

This command displays statistics for a specified PPTP tunnel session.

Syntax

```
show pptp tunnel <number> session <number>
```

- **Remote call id**—Session identifier for this control channel tunnel.
- **Peer Name**—Peer session name on this interface—typically the login name of the remote user.
- **Session Duration**—Number of milliseconds the session has been up on this interface.
- **Line state**—Current status of the control tunnel: *Allocated, Waiting, Calling, Offering, Answering, Connected, Disconnecting Local, Disconnecting Remote, Lost*
- **Call device number**—Logical device the L2TP stack uses internally; useful for debugging purposes.
- **Call serial number**—Serial number applied to the session.
- **Connect BPS**—Baud rate at which this session was established.
- **Call bearer type**—Bearer type for this session: *Analog or Digital*
- **Session frame type**—Framing type for this session: *Asynchronous or Synchronous*
- **Local receive packet window**—Local send window size for this session.
- **Remote receive packet window**—Remote send window size for this session.
- **Remote window type**—Indicates whether windowing (sequencing of L2TP packets) is enabled or disabled on the remote side of the tunnel.
- **Local window type**—Indicates whether windowing (sequencing of L2TP packets) is enabled or disabled on the local side of the tunnel.
- **Data tunnel receive packets**—Sum of data packets received on the data tunnel for this session.
- **Data tunnel receive packets with data**—Sum of packets received on the data tunnel for this session which contained data.
- **Processed data tunnel receive packets**—Sum of packets received on the data tunnel for this session which were processed.
- **In sequence data tunnel receive packets**—Sum of packets received in sequence on the data tunnel for this session.

- **Out of sequence data tunnel receive packets**—Sum of packets received out of sequence on the data tunnel for this session.
- **In order data tunnel receive packets**—Sum of packets received in order on the data tunnel for this session.
- **Out of order data tunnel receive packets**—Sum of packets received out of order on the data tunnel for this session.
- **Flow discarded data tunnel receive packets**—Sum of packets received on the data tunnel for this session which were discarded due to flow control.
- **Out of order discarded data tunnel receive packets**—Sum of packets received on the data tunnel for this session which were discarded due to ordering.
- **Data tunnel send packets**—Sum of packets transmitted on the data tunnel for this session.
- **Data tunnel send packets with data**—Sum of packets transmitted on the data tunnel for this session containing data.
- **Data tunnel send packets without data**—Sum of zero length packets transmitted on the data tunnel for this session.
- **Data tunnel flow control timeouts**—Sum of flow control timeouts experienced on the data tunnel for this session.
- **Local data tunnel flow control on**—Current state of local flow control for this data tunnel session.
- **Local data tunnel flow control enables**—Sum of local flow control enables for this data tunnel session.
- **Remote data tunnel flow control on**—Current state of remote flow control for this data tunnel session.
- **Remote data tunnel flow control enables**—Sum of remote flow control enables for this data tunnel session.
- **Data tunnel reassembly timeout**—Sum of re-assembly timeouts for this data tunnel session.

Related Commands

[`list pptp tunnel <number> sessions`](#)

[`list pptp tunnels`](#)

[`show pptp tunnel`](#)

L2TP

add l2tp lns <1 to 9> address <IP address> This command adds a local L2TP network server (LNS) and its associated IP address on the LAC (L2TP Access Concentrator) side of the L2TP tunnel. Additional security and a shared secret may also be specified using the set L2TP lns command.

The LNS is added to a list of default LNS systems that the LAC may seek to contact due to failure to receive an LNS tunnel endpoint (IP address) from the RADIUS server. A failure could be caused by an unconfigured RADIUS server, or a complete absence of the value in the user's RADIUS profile.

Syntax

```
add l2tp lns <1 to 9> address <IP address>
```

Related Commands

[delete l2tp lns](#)

[disable l2tp lns](#)

[enable l2tp lns](#)

[list l2tp lns](#)

[set l2tp lns](#)

[show l2tp lns](#)

delete l2tp lns This command removes a local l2tp network server (LNS) from the LAC side of the l2tp tunnel created with the [add l2tp lns <1 to 9> address <IP address>](#) command.

Syntax

```
delete l2tp lns <1 to 9>
```

Related Commands

[DNS](#)

[disable l2tp lns](#)

[enable l2tp lns](#)

[list l2tp lns](#)

[set l2tp lns](#)

[show l2tp lns](#)

**disable l2tp
lcp_renegotiation_
at_lns**

When LCP renegotiation is disabled, and the local router card is the LNS, it only performs renegotiation when needed.

Syntax

```
disable l2tp lcp_renegotiation_at_lns
```

disconnect l2tp tunnel

This command disconnects the specified L2TP tunnel, bringing down all sessions running in the tunnel.

Syntax

```
disconnect l2tp tunnel <number>
```

Related Commands

[list l2tp tunnels](#)

[list l2tp sessions tunnel](#)

[show all l2tp tunnels](#)

**disconnect l2tp tunnel
<number> session
<number>**

This command brings down the specified call running in the L2TP tunnel. When the last session is brought down, the tunnel comes down with it. See the [list l2tp tunnels](#) command to view tunnel session information.

Syntax

```
disconnect l2tp tunnel <number> session <number>
```

Related Commands

[list l2tp sessions tunnel](#)

[show all l2tp tunnels](#)

[list l2tp tunnels](#)

disable l2tp lns

This command prevents the specified router card from receiving tunnel requests as an L2TP network server (LNS). The default is enabled.

Syntax

```
disable l2tp lns <1 to 9>
```

Related Commands

[DNS](#)

[delete l2tp lns](#)

[enable l2tp lns](#)

[list l2tp lns](#)

[set l2tp lns](#)

enable l2tp lns This command enables the specified router card to receive tunnel requests as an L2TP network server (LNS). See the [delete l2tp lns](#) command for more information. The default is enabled.

Syntax

```
enable l2tp lns <1 to 9>
```

Related Commands

[delete l2tp lns](#)

[disable l2tp lns](#)

[list l2tp lns](#)

[set l2tp lns](#)

[show l2tp lns](#)

enable l2tp lcp_renegotiation_at_lns When LCP renegotiation is enabled, the local router card is the LNS it will always performs renegotiation.

Syntax

```
enable l2tp lcp_renegotiation_at_lns
```

Related Commands

[delete l2tp lns](#)

[disable l2tp lns](#)

[list l2tp lns](#)

[set l2tp lns](#)

[show l2tp lns](#)

list l2tp lns This command displays settings of all L2TP network servers (LNS) configured with the [add l2tp lns <1 to 9> address <IP address>](#) command. It lists the following information.

Syntax

```
list l2tp lns
```

- **Index**—Number corresponding to particular L2TP network server in the Local L2TP LNS table.
- **Address**—Address of particular L2TP network server in the table.

Related Commands

[delete l2tp lns](#)

[disable l2tp lns](#)

[enable l2tp lns](#)

[set l2tp lns](#)

[show l2tp lns](#)

list l2tp tunnels This command displays settings on the L2TP network server (LNS) for all configured L2TP tunnels. See the [list connections](#) command for DLL settings on the L2TP area concentrator (LAC).

Syntax

```
list l2tp tunnels
```

- **Tun(nel) ID**—Designation of the L2TP tunnel
- **Status**—State of the tunnel. Values displayed are *NO STATE*, *ALLOCATED*, *CONNECTING*, *STARTING SESSION*, *ESTABLISHED*, *STOPPING SESSION*, *DISCONNECTING*, *LOST*, or *IDLE TIMEOUT*
- **IP address**—IP address of the remote tunnel endpoint to which it is connected. Depending on the RAS executing the command, if looking at the LNS, this value is the LAC address.

Related Commands

[list connections](#)

[disconnect l2tp tunnel](#)

[list l2tp sessions tunnel](#)

[show all l2tp tunnels](#)

list l2tp sessions tunnel This command displays information on all configured L2TP tunnel sessions.

Syntax

```
list l2tp sessions tunnel <number>
```

- **Tun(nel) ID**—Designation of the L2TP pipe.
- **Ses(sion) ID**—Designation of the L2TP session.
- **Status**—Status of the tunnel session. Values displayed are *NO STATE*, *ALLOCATED*, *WAITING*, *CALLING*, *OFFERING*, *ANSWERING*, *CONNECTED*, *DISCONNECTING LOCAL*, *DISCONNECTING REMOTE*, or *LOST CONTROL TUNNEL*.
- **User Name**—Designation of user active on this tunnel session.

Related Commands

[disconnect l2tp tunnel](#)

[list l2tp tunnels](#)

[show all l2tp tunnels](#)

list l2tp session_counters This command displays statistics for configured L2TP tunnels.

Syntax

```
list l2tp session_counters
```

- **Tunnel Endpoint**—the IP address of the tunnel endpoint.
- **No of Successful Attempts**—Number of connection attempts that succeeded.
- **No of Failed Attempts**—Number of connection attempts that failed.
- **Total Number of Attempts**—Total number of successful and failed connection attempts.

reset l2tp session_counters This command resets the L2TP session counters back to zero.

Syntax

```
reset l2tp session_counters
```

set l2tp This command configures default L2TP tunnel attributes on the router card. These values can be overridden by RADIUS. L2TP tunnels can also be enabled locally using the [set tunnel user](#) command.

Syntax

```
set l2tp
    ack_timeout <milliseconds>
    control_receive_packet_window <number>
    data_receive_packet_window <number>
    flow_control [enable | disable]
    load_balancing [enable | disable]
    loglevel [disable | control_pkt_only |
    ctrl_and_headers_of_data_pkt | ctrl_and_data_pkt]
    max_sessions <number>
    max_tunnels <number>
    num_echo_retransmission_interval <number>
    num_retransmissions <number>
    num_retransmissions_control <number>
    num_terminators <number>
    reassembly_timeout <milliseconds>
    reply_timeout <number>
    retransmission_interval <seconds>
    retransmission_interval_control <number>
    tunnel_challenge_incoming [enable | disable]
    tunnel_challenge_outgoing [enable | disable]
    tunnel_password_encryption_style [no_salt | with_salt]
```

Table 155 Set L2TP Command Parameters Descriptions

Parameter	Description
ack_timeout	Number of milliseconds the L2TP facility waits to send and acknowledge to its peer when there is no data or control packets to piggyback the acknowledgment to. The default causes immediate acknowledgment when no data or control packets are pending. Recommended value 500 to 600. The default is 500.
control_receive_packet_window	Size in number of packets of the control channel receive window sent to the L2TP facility's peers. After this number of control packets is acknowledged as received by the L2TP client, more packets are transmitted by the L2TP server. The default is 7.
data_receive_packet_window	Size in number of packets of the data channel receive window sent to the L2TP facility's peers. After this number of data packets is acknowledged as received by the L2TP client, more packets are transmitted by the L2TP server. The default is 0.
flow_control	Enables/disables data tunnel flow control. The default is disable.

Table 155 Set L2TP Command Parameters Descriptions

Parameter	Description
load_balancing	When enabled, the router card accesses least-used LNS over the last 60 seconds. The default is enable.
loglevel	Logging level to set to dump packets to the Console. The default is disable.
max_sessions	Maximum number of simultaneous active sessions the router card can support. The limit is 465. The range is 1 to 465.
max_tunnels	Maximum number of simultaneous active tunnels the router card can support. The limit is 780.
num_retransmissions	Number of retransmissions the L2TP facility tries before assuming its peer is unreachable. The default causes the stack to not try retransmissions. The default is 0.
num_terminators	Number of concurrent tunnels the router card can <i>initiate</i> at one time. But, the router card can maintain up to 256 concurrent tunnels. Limit and The default is 64.
reassembly_timeout	Number of milliseconds the L2TP facility uses to determine the window to use before reassembling out of order packets. A low value increases the chance out-of-sequence packets will be lost (which MAY cause the PPP decompression engine to reset), a high value increases the time period where the L2TP stack processes packets which were received out of order (especially in the case of a packet which was lost within the network). The default may cause all out of sequence packets to be lost. The default is 0.
reply_timeout	Number of seconds the L2TP facility waits until a timeout occurs in receiving a response to the keep-alive (hello) message. The default is 0.
retransmission_interval	Period in seconds between retransmissions of control packets which haven't been acknowledged. The default is 10 seconds.
tunnel_challenge_incoming	LNS asks LAC for authentication. If enabled, only authenticated tunnel requests are honored. The default is disabled. When disabled, requires all incoming tunnels to perform authentication
tunnel_challenge_outgoing	If enabled, the LAC sends a tunnel challenge to the LNS if a shared secret is present. If disabled, the LAC does not send a tunnel challenge. The default is disabled.
tunnel_password_encryption_style	This parameter determines whether or not to use salt password encryption when negotiating the tunnel password with the RADIUS server. If your RADIUS server uses salt encryption you should set this parameter to use salt. no_salt—Do not use salt password encryption. This is the default. with_salt—Use salt password encryption.

Related Commands

[set tunnel user](#)

set l2tp lns This command sets parameters for the specified l2tp network server created by the [add l2tp lns <1 to 9> address <IP address>](#) command.

Syntax

```
set l2tp lns <l2tp server number>
```

```
shared_secret <string>
security_level [none | control | data | both]
```

Table 156 Set L2TP LNS Command Parameters Descriptions

Parameter	Description
<l2tp server number>	The indexed value for the specified L2TP network server. The range is 1 to 9.
shared_secret	The password shared by the L2TP network server and access concentrator (LAC). The limit is 256 ASCII characters.
security_level	The degree of HMAC-MD5 packet encryption the L2TP network server will perform: data—encryption for data packets only control—encryption for data packets only both—encryption for data and control packets none—no encryption performed. Default

Related Commands

[add l2tp lns <1 to 9> address <IP address>](#)

[delete l2tp lns](#)

[disable l2tp lns](#)

[enable l2tp lns](#)

[list l2tp lns](#)

[show l2tp lns](#)

show l2tp settings This command displays settings for configured L2TP tunnels. Also see the [DNS](#) and [set l2tp lns](#) commands.

Syntax

```
show l2tp settings
```

- **Maximum Number of Sessions**—Maximum number of simultaneous active sessions L2TP supports. The maximum is 465.
- **Maximum Number of Tunnels**—Maximum number of simultaneous active tunnels L2TP will support. Since sessions are multiplexed within a single tunnel, this value displays the number of L2TP tunnels supported *per tunnel*.
- **Number of Control Channel Seek Descriptor**—Number of tunnel terminators L2TP can simultaneously connect to.
- **Flow Control**—Indicates whether L2TP uses flow control on the data tunnel. The default is disabled.

- **Data Channel Delayed Acknowledgement Timeout**—Interval in milliseconds L2TP will wait to send acknowledge its peer when there are no data or control packets to piggyback the acknowledge to. The default is 500.
- **Data Channel Reassembly Timeout**—Interval in milliseconds L2TP uses to determine the window to use before reassembling out-of-order packets. A low value increases the chance that out-of-sequence packets will be lost. A high value increases the period when L2TP processes packets received out of order. The default of 0 may drop all out-of-sequence packets.
- **Control Channel Receive Packet Window**—Size of the control channel receive buffer awaiting acknowledgment by the system's peers. The default is 7.
- **Data Channel Receive Packet Window**—Size of the data channel receive buffer awaiting acknowledgment by the system's peers. The default is 7.
- **Inactivity Idle Timeout**—Interval in seconds L2TP will wait inactively and send a Hello packet. The default is 0.
- **Echo reply timeout**—Interval in seconds L2TP waits until a time-out occurs in receiving a response to the Hello message.
- **Logging Level**—The logging level L2TP is set to. Choices: *Disabled*, *Control Packets*, *Control and Data Packet Headers and Control and Data Packets*.
- **Load balance status**—Indicates whether load balancing is enabled or disabled.
- **Number of Retransmissions**—Number of retransmissions L2TP will try before assuming its peer is unreachable. The default value of 0 cause L2TP to stop retransmissions. The maximum is 3.
- **Retransmission Interval**—Interval in seconds between retransmissions.
- **Tunnel Challenge**—When enabled requires all incoming tunnels to perform encryption. The default is disabled.
- **L2TP Lns**—L2TP Lns support.
- **Tunnel Password Encryption Style**—Whether or not to use salt password encryption when negotiating the tunnel password with the RADIUS server.
- **LCP Renegotiate at LNS**—This has meaning only at the LNS. When disabled, the router card acting as the LNS attempts renegotiation only if a need arises. When it is enabled, LCP renegotiation is always attempted. The default is disabled.

Related Commands

[set l2tp lns](#)

show l2tp counters This command displays the l2tp counters.

Syntax

```
show l2tp counters
```

Example

```
show l2tp counters
```

show l2tp lns This command displays settings for a local LNS entry on the LAC side of a L2TP tunnel.

Syntax

```
show l2tp lns <number>
```

Related Commands

[delete l2tp lns](#)

[disable l2tp lns](#)

[enable l2tp lns](#)

[list l2tp lns](#)

[set l2tp lns](#)

show l2tp tunnel This command displays statistics of the specified L2TP tunnel.

Syntax

```
show l2tp tunnel <number>
```

- **Local control tunnel ID**—Identifier of the specified local control tunnel
- **Peer control tunnel ID**—Identifier of the specified remote control tunnel
- **Control tunnel state**—Current status of the specified control tunnel
- **Local init connection**—Indicates whether tunnel was established locally or not
- **IP address**—Remote peer's IP address
- **Local receive packet window**—Size of local send window
- **Remote receive packet window**—Size of remote receive window
- **Control tunnel receive packets**—Sum of control packets received on the control tunnel
- **Control tunnel receive packets with data**—Sum of control packets received with data
- **Control tunnel receive packets without data**—Sum of zero length packets received

- **Processed control tunnel receive packets**—Sum of receive packets that were processed
- **In sequence control tunnel receive packets**—Sum of packets received in sequence
- **Out of sequence control tunnel receive packets**—Sum of packets received out of sequence
- **In order control tunnel receive packets**—Sum of packets received in order
- **Out of order control tunnel receive packets**—Sum of packets received out of order
- **Flow discarded control tunnel receive packets**—Sum of received packets discarded due to flow control
- **Out of order discarded control channel receive packets**—Sum of received packets discarded due to ordering
- **Control tunnel send packets**—Sum of packets transmitted
- **Control tunnel send packets with data**—Sum of packets transmitted with data
- **Control tunnel send packets without data**—Sum of zero length packets transmitted
- **Control tunnel flow control timeouts**—Sum of timeouts caused by flow control
- **Control tunnel flow control on**—Status of local flow control: **enabled** or **disabled**
- **Local control tunnel flow control enables**—Sum of local flow control enables for the control session
- **Remote control tunnel flow control on**—Status of remote flow control: **enabled** or **disabled**
- **Remote control tunnel flow control enables**—Sum of remote flow control enables for the control session
- **Control tunnel reassembly timeouts**—Sum of reassembly timeouts
- **Remote host name**—Host name of the L2TP peer

show l2tp tunnel
<number> session
<number>

This command displays statistics for a specified L2TP tunnel session.

Syntax

```
show l2tp tunnel <number> session <number>
```

- **Remote call id**—Session identifier for this control channel tunnel
- **Peer Name**—Peer session name on this interface—typically the login name of the remote user
- **Session Duration**—Number of milliseconds the session has been up on this interface
- **Line state**—Current status of the control tunnel: *Allocated, Waiting, Calling, Offering, Answering, Connected, Disconnecting Local, Disconnecting Remote, Lost*
- **Call device number**—Logical device the L2TP stack uses internally; useful for debugging purposes.
- **Call serial number**—Serial number applied to the session
- **Connect BPS**—Baud rate this session was established at
- **Call bearer type**—Bearer type for this session: *Analog* or *Digital*
- **Session frame type**—Framing type for this session: *Asynchronous* or *Synchronous*
- **Local receive packet window**—Local send window size for this session
- **Remote receive packet window**—Remote send window size for this session
- **Remote window type**—Indicates whether windowing (sequencing of L2TP packets) is enabled or disabled on the remote side of the tunnel
- **Local window type**—Indicates whether windowing (sequencing of L2TP packets) is enabled or disabled on the local side of the tunnel
- **Data tunnel receive packets**—Sum of data packets received on the data tunnel for this session
- **Data tunnel receive packets with data**—Sum of packets received on the data tunnel for this session which contained data
- **Processed data tunnel receive packets**—Sum of packets received on the data tunnel for this session which were processed
- **In sequence data tunnel receive packets**—Sum of packets received in sequence on the data tunnel for this session
- **Out of sequence data tunnel receive packets**—Sum of packets received out of sequence on the data tunnel for this session
- **In order data tunnel receive packets**—Sum of packets received in order on the data tunnel for this session
- **Out of order data tunnel receive packets**—Sum of packets received out of order on the data tunnel for this session

- **Flow discarded data tunnel receive packets**—Sum of packets received on the data tunnel for this session which were discarded due to flow control
- **Out of order discarded data tunnel receive packets**—Sum of packets received on the data tunnel for this session which were discarded due to ordering
- **Data tunnel send packets**—Sum of packets transmitted on the data tunnel for this session
- **Data tunnel send packets with data**—Sum of packets transmitted on the data tunnel for this session containing data
- **Data tunnel send packets without data**—Sum of zero length packets transmitted on the data tunnel for this session
- **Data tunnel flow control timeouts**—Sum of flow control timeouts experienced on the data tunnel for this session
- **Local data tunnel flow control on**—Current state of local flow control for this data tunnel session
- **Local data tunnel flow control enables**—Sum of local flow control enables for this data tunnel session
- **Remote data tunnel flow control on**—Current state of remote flow control for this data tunnel session
- **Remote data tunnel flow control enables**—Sum of remote flow control enables for data tunnel session
- **Data tunnel reassembly timeout**—Sum of re-assembly timeouts for this data tunnel session

**enable L2TP
force_multiple_tunnels**

By default, one tunnel is established between a LAC and an LNS. Multiple users on the LAC using the same LNS share a single tunnel between the LAC and LNS.

When L2TP `force_multiple_tunnels` is enabled, it over-rides the default and a separate tunnel is established between the LAC and LNS for each user, creating multiple tunnels.

Syntax

```
enable L2TP force_multiple_tunnels
```

**disable L2TP
force_multiple_tunnels**

To return to the default mode of single-tunnel usage for multiple users on the LAC sharing an LNS, enter the `disable L2TP force_multiple_tunnels` command.

Syntax

```
disable L2TP force_multiple_tunnels
```

**enable L2TP
use_client_auth_id_for_
assignment_id**

When multiple users on an LAC connecting to the same LNS exist, these users are grouped into tunnels. By default, users are grouped based on `assignment_id`. Refer to the `set tunnel user <user_name> assignment_id` command for more information.

When L2TP `use_client_auth_id_for_assignment_id` is enabled, users are grouped into tunnels based on client `authorization_id` (instead of `assignment_id`).

Syntax

```
enable L2TP use_client_auth_id_for_assignment_id
```

**disable L2TP
use_client_auth_id_for_
assignment_id**

To return to the default mode of using `authorization_id` to group users into tunnels, enter the `disable L2TP use_client_auth_id_for_assignment_id` command.

Syntax

```
disable L2TP use_client_auth_id_for_assignment_id
```

PPTP

set pptp <number> This command configures flow characteristics for a PPTP tunnel on the router card. PPTP tunnels can also be enabled locally using the [set tunnel user](#) command.

Syntax

```
set pptp <number>
    data_channel_delayed_ack_timeout <milliseconds>
    data_channel_reassembly_timeout <milliseconds>
    data_channel_receive_packet_window <number>
    echo_reply_timeout <seconds>
    flow_control [enable | disable]
    idle_timeout <number>
    load_balancing [enable | disable]
    loglevel [disable | control_pkt_only |
    ctrl_and_headers_of_data_pkt | ctrl_and_data_pkt]
    max_seek_descriptors <number>
    max_sessions <number>
    max_tunnels <number>
```

Table 157 Set PPTP Command Parameters Descriptions

Parameter	Description
<number>	Stack index number.
data_channel_delayed_ack_timeout	Number of milliseconds the PPTP stack waits to send and acknowledge to its peer when there is no data packets to piggyback the acknowledgment to. The default causes immediate acknowledgment when no data packets are pending. The default is 0.
data_channel_reassembly_timeout	Number of milliseconds the stack uses to determine the window to use before reassembling out of order data packets. A low value increases the chance out-of-sequence packets will be lost (which MAY cause the PPP decompression engine to reset), a high value increases the time period where the pptp stack processes packets which were received out of order (especially in the case of a packet which was lost within the network). The default may cause all out of sequence packets to be lost. The default is 0.
data_channel_receive_packet_window	Size in number of packets of the data channel receive window sent to the stack's peers. The range is 0-256.
echo_reply_timeout	Number of seconds the PPTP stack waits until a timeout occurs in receiving a response to the keep-alive (hello) message. The default is 0.
flow_control	Enables/disables data tunnel flow control. The default is Disable.
idle_timeout	Interval in seconds waited before the control tunnel is timed out. The range is 0-65535.

Table 157 Set PPTP Command Parameters Descriptions

Parameter	Description
load_balancing	When enabled, the router card accesses least-used LNS over the last 60 seconds. The default is Enable.
loglevel	Logging level to set to dump packets to the console. The default is Disable.
max_sessions	Maximum number of simultaneous active sessions the stack can support. The default is 0. The range is 1-451.
max_seek_descriptors	Highest number of tunnel endpoints the PPTP stack can remain simultaneously connected to. The range is 1-451. The default is 8.
max_tunnels	Maximum number of simultaneous active tunnel sessions per tunnel the stack can support. The range is 1-451.

Related Commands

[set tunnel user](#)

**add pptp pns <1-9>
address <IP address>**

This command adds a local PPTP network server (PNS) from the client (PAC) side of the PPTP tunnel.

Syntax

```
add pptp pns <1 to 9> address <IP address>
```

show pptp settings This command displays settings for configured PPTP tunnels.

Syntax

```
show pptp settings
```

- **Maximum Number of Sessions**—Maximum number of simultaneous active sessions PPTP supports.
- **Maximum Number of Tunnels**—Maximum number of simultaneous active tunnels PPTP will support. Since sessions are multiplexed within a single tunnel, this value displays the number of PPTP tunnels supported *per tunnel*.
- **Number of Control Channel Seek Descriptor**—Number of tunnel terminators PPTP can simultaneously connect to. The default is **8**.
- **Authentication Type**—Whether PPTP seeks encryption from its peers. The default is **Disabled**.
- **Flow Control**—Whether PPTP uses flow control on the data tunnel. The default is **enabled**.
- **Data Channel Delayed Acknowledgement Timeout**—Interval in milliseconds PPTP will wait to send acknowledge its peer when there are no data or control packets to piggyback the acknowledge to. The default is **500**.
- **Data Channel Reassembly Timeout**—Interval in milliseconds PPTP uses to determine the window to use before reassembling out-of-order packets. A low value increases the change that out-of-sequence packets will be lost. A high value increases the period when PPTP processes packets received out of order. The default of 0 may drop all out-of-sequence packets.
- **Control Channel Receive Packet Window**—Size of the control channel receive window sent to PPTP's peers. The default is **7**.
- **Data Channel Receive Packet Window**—Size of the data channel receive window sent to PPTP's peers. The default is **7**.
- **Inactivity Idle Timeout**—Interval in seconds PPTP will wait inactively and send a Hello packet. The default is **0**.
- **Echo reply timeout**—Interval in seconds PPTP waits until a time-out occurs in receiving a response to the Hello message.
- **Load balance status**—Whether load balancing is **enabled** or **disabled**.
- **Logging Level**—The logging level PPTP is set to. Choices: *Disabled, Control Packets, Control and Data Packet Headers and Control and Data Packets*.
- **Pptp Pns**—Displays the state of PPTP network server support.

delete pptp pns This command removes a local PPTP network server (PNS) from the client (PAC) side of the PPTP tunnel created with the `add pptp pns` command.

Syntax

```
delete pptp pns <1 to 9>
```

Related Commands

[add pptp pns](#)

enable pptp pns This command enables PPTP network server support. The default is enabled.

Syntax

```
enable pptp pns
```

Related Commands

[disable pptp pns](#)

[show pptp settings](#)

disable pptp pns This command disables the specified PPTP network server.

Syntax

```
disable pptp pns
```

Related Commands

[enable pptp pns](#)

[show pptp settings](#)

disconnect pptp tunnel <number> This command disconnects the specified PPTP tunnel, bringing down all sessions running in the tunnel.

Syntax

```
disconnect pptp tunnel <number>
```

Related Commands

[list pptp tunnel <number> sessions](#)

[list pptp tunnels](#)

[show pptp tunnel](#)

[show pptp tunnel <number> session <number>](#)

**disconnect pptp
<number> session
<number>**

This command brings down the specified call running in the PPTP tunnel. When the last session is brought down, the tunnel comes down with it. See the [list pptp tunnels](#) command to view tunnel session information.

Syntax

```
disconnect pptp <number> session <number>
```

Related Commands

[list pptp tunnel <number> sessions](#)

[list pptp tunnels](#)

[show pptp tunnel](#)

[show pptp tunnel <number> session <number>](#)

list pptp pns

This command displays settings of all PPTP network servers configured with the [add pptp pns <1-9> address <IP address>](#) command.

Syntax

```
list pptp pns
```

- **Index**—Number corresponding to particular PPTP Network Server in the LOCAL PPTP PNS Table.
- **address**—Address of particular PPTP Network Server in the table.

Related Commands

[add pptp pns <1-9> address <IP address>](#)

**list pptp tunnel
<number> sessions**

This command displays information on all current PPTP tunnel sessions.

Syntax

```
list pptp tunnel <number> sessions
```

- **Tun(nel) ID**—Designation of the PPTP pipe.
- **Ses(sion) ID**—Designation of the PPTP session.
- **Status**—Status of the tunnel session. Values displayed are *NO STATE*, *ALLOCATED*, *WAITING*, *CALLING*, *OFFERING*, *ANSWERING*, *CONNECTED*, *DISCONNECTING LOCAL*, *DISCONNECTING REMOTE*, or *LOST CONTROL TUNNEL*.
- **User Name**—Designation of user active on this tunnel session.

Related Commands

[disconnect pptp tunnel <number>](#)
[disconnect pptp <number> session <number>](#)
[list pptp tunnel <number> sessions](#)
[list pptp tunnels](#)
[show pptp tunnel](#)
[show pptp tunnel <number> session <number>](#)

list pptp tunnels This command displays settings for all current PPTP tunnels.

Syntax

```
list pptp tunnels
```

- **Tun(nel) ID**—designation of the PPTP tunnel.
- **Status**—state of the tunnel. Values displayed are *NO STATE*, *ALLOCATED*, *CONNECTING*, *STARTING SESSION*, *ESTABLISHED*, *STOPPING SESSION*, *DISCONNECTING*, *LOST*, or *IDLE TIMEOUT*.
- **IP address**—IP address of the remote tunnel endpoint to which it is connected. Depending on the RAS executing the command, if looking at the PNS, this value is the LAC address.

Related Commands

[disconnect pptp tunnel <number>](#)
[list pptp tunnel <number> sessions](#)
[show pptp tunnel](#)
[show pptp tunnel <number> session <number>](#)

Tunnel Switch

enable tunnel switch This command enables tunnel switching on a global box-wide basis.

Syntax

```
enable tunnel switch
```

disable tunnel switch This command disables tunnel switching on a global box wide basis.

Syntax

```
disable tunnel switch
```

**show tunnel
switch_counters**

This command shows the following tunnel switch counters.

Syntax

```
show tunnel switch_counters
```

- Number of total PPTP Tunnels switched to PPTP
- Number of total PPTP tunnel switched to L2TP
- Number of total L2TP tunnel switched to PPTP
- Number of total L2TP tunnel switched to L2TP
- Number of current PPTP tunnel switched to L2TP
- Number of current PPTP tunnel switched to PPTP
- Number of current L2TP tunnel switched to PPTP
- Number of current L2TP tunnel switched to L2TP

**show tunnel_switch
settings**

This command shows the current configuration settings for the tunnel switch.

Syntax

```
show tunnel_switch settings
```

VTP

enable vtp timestamp checking This command enables time stamp checking for Virtual Tunnel Protocol (VTP) control packets.

Syntax

```
enable vtp timestamp checking
```

disable vtp timestamp checking This command disables time stamp checking for Virtual Tunnel Protocol (VTP) control packets.

Syntax

```
disable vtp timestamp checking
```

disconnect vtp tunnel This command disconnects a Virtual Tunnel Protocol (VTP) tunnel with the designated tunnel-ID.

Syntax

```
disconnect vtp tunnel <0 to 4294967295>
```

list vpn <0 to 65535> vtp tunnels This command lists all VTP tunnels belonging to the given VPN-Id.

Syntax

```
list vpn <0 to 65535> vtp tunnels
```

list vtp tunnels This command displays settings for all current VTP tunnels.

Syntax

```
list vtp tunnels
```

- **TunnelId**—the unique id for a VTP tunnel established between NAS and VPNGW.
- **VpnName**—the Name for a VPN that the user is connected to.
- **PeerIpAddress**—This will point to the NAS on VPNGW and shall point to VPNGW on NAS.



SECURITY COMMANDS

This chapter describes the following Security Commands:

- [AAA Server](#)
- [Authentication Commands](#)
- [CBCP Commands](#)
- [IPsec \(Policy\) Commands](#)
- [IPsec \(IP Security\) Commands](#)
- [Microsoft Point to Point Encryption Commands](#)
- [Network Address Translation Commands](#)
- [Packet Filtering Commands](#)
- [RADIUS](#)
- [Security Association](#)
- [TACACS+](#)

AAA Server

This section covers commands that add, delete, and modify elements of authentication, authorization, and accounting (AAA).

add aaa_server

This command specifies a remote server to use by adding an AAA server name to the AAA Domain Table to support AAA. The AAA domain table lists all domains a user can log in to. A preference number is assigned to AAA names in the DNS table where IP address resolution is performed according to highest preference first.

Syntax

```
add aaa_server <name>
    aaa_type [auth | acco]
    address <IP address>
    enabled [yes | no]
    encryption [off | on]
    mask <string>
    port <port>
    preference <1 to 99>
    retransmit <0 to 65535>
```

```

secret <string16_and_null>
server_name <string>
timeout <1 to 60>
passthru [disabled | enable]

```

Table 158 Add AAA_Server Command Parameters Descriptions

Parameter	Description	Settings
<name>	A name for the AAA server. Example: joe@smith.com.	Up to 64 ASCII characters.
aaa_type	The type of AAA server assigned.	acco—accounting server auth—authentication server
address	The IP address of the AAA server. The default IP address is 0.0.0.0.	xxx.xxx.xxx.xxx
enabled	The state of the AAA server. The server is enabled by default.	yes no
encryption	The encryption state of entire data packet. This is valid only for TACACS+ which encrypts the body of the message. Encryption is turned off by default.	on off
mask	This is an alphanumeric string. It is scanned to obtain the mask setting wanted by the user.	Up to 20 ASCII characters.
port	The port number on the AAA server. The TACACS+ standard port number is 49.	1 to 65535
preference	This field is the preference number assigned to a Server in the DNS table. It defines the sequence in which the hosts will be used. The lower the number value, the higher the preference.	1 to 99
retransmit	The number of retransmissions or retry count.	0 to 65535
secret	The password shared by AAA server and the router card for encryption. This field can be left blank or filled with null character ("").	Up to 15 ASCII characters.
server_name	Familial name for the AAA server to be identified by DNS.	Up to 64 ASCII characters.
timeout	The timeout value for trying the next server.	0 to 60
passthru	The setting of the passthru setting.	enable disable

Related Commands

[delete aaa_server](#)

[list aaa_server](#)

[set aaa_server](#)

[show aaa_server <name> preference <number>](#)

delete aaa_server This command removes the TACACS+ server created with the [add aaa_server](#) command.

Syntax

```
delete aaa_server <name>
```

Example

```
delete aaa_server bostonacct2
```

Related Commands

[add aaa_server](#)

[list aaa_server](#)

[set aaa_server](#)

[show aaa_server <name> preference <number>](#)

delete aaa_server <name> preference <number> This command deletes an AAA server with the specified name and preference from the AAA domain table.

Syntax

```
delete aaa_server <name> preference <number>
```

Example

```
delete aaa_server bostonacct2 preference 2
```

list aaa_server This command displays information of TACACS+ servers, including AAA name, preference, IP address, and state.

Syntax

```
list aaa_server
```

Example

```
list aaa_server
```

Related Commands

[add aaa_server](#)

[delete aaa_server](#)

[set aaa_server](#)

[show aaa_server <name> preference <number>](#)

set aaa_server This command edits a TACACS+ server created with the [add aaa_server](#) command.

Syntax

```
set aaa_server <name>
    address <IP address>
    enabled [yes | no]
    encryption [off | on]
    port <0 to 65535>
    preference <0 to 99>
    retransmit <0 to 65535>
    secret <string>
    server_name <string>
```

Table 159 Set AAA_Server Command Parameters Descriptions

Parameter	Description	Settings
<name>	The name of the AAA server.	Up to 64 ASCII characters.
address	The IP address of the AAA server. The default IP address is 0.0.0.0.	xxx.xxx.xxx.xxx
enabled	Toggles the AAA server on or off. The server is enabled by default.	yes no
encryption	The encryption state of entire data packet. This is valid only for TACACS+ which encrypts the body of the message. Encryption is turned off by default.	on off
port	The port number on the AAA server.	0 to 65535
preference	This field is the preference number assigned to a Server in the DNS table. It defines the sequence in which the hosts will be used. The lower the number value, the higher the preference.	1 to 99
retransmit	The number of retransmissions or retry count.	0 to 65535
secret	The shared secret between TACACS+ server and NAS. Note: RADIUS uses this only for the password and TACACS+ uses this for the whole body of the message.	Up to 16 ASCII characters.
server_name	The name of the AAA host to be resolved by DNS.	Up to 64 ASCII characters.

Related Commands

[add aaa_server](#)

[delete aaa_server](#)

[list aaa_server](#)

[show aaa_server <name> preference <number>](#)

show aaa_server
<name> preference
<number>

This command shows the current settings for the specified server configured with the [add aaa_server](#) command.

Syntax

```
show aaa_server <name> preference <number> settings
```

Table 160 Show AAA_Server Parameter Descriptions

Parameter	Description	Settings
Name	The name of the AAA server	Up to 32 ASCII characters.
Preference	This field is the preference number assigned to a server in the DNS table. It defines the sequence.	1 to 10

Related Commands

[delete aaa_server](#)

[list active interfaces](#)

[set aaa_server](#)

Authentication Commands

This section covers commands used to control authentication through the CLI.

disable authentication This command disables specific types of authentication.

Syntax

```
disable authentication [local | remote | hint_assigned |
send_auth_service_type]
```

Table 161 Disable Authentication Parameters Descriptions

Parameter	Description
local	User authentication based on a password specified in the User Table. When you issue the <code>add user</code> command, entering a password activates local authentication. If no password is specified (passwords are optional), and remote authentication is not enabled, the user is not able to establish a connection. Local authentication is enabled globally by default.
remote	Authentication based on a password specified in a RADIUS or TACACS+ server.
hint_assigned	Remote authentication employing optional IP address assignment. The router card automatically assigns a temporary IP address to every dial-in user and reports it with the Framed-IP-Address in the RADIUS authentication request record. The RADIUS server may choose to accept this IP address with an Authentication-Ack message or choose to assign another IP address with an Authentication-Ack message containing no Frame-IP-Address field. The default is disabled.
send_auth_service_type	Disables the sending of the service type to the RADIUS server. The default is enabled.



Local authentication takes precedence over remote authentication.

Example

```
disable authentication remote
```

Related Commands

[enable authentication](#)

[set authentication](#)

enable authentication This command enables specific types of authentication.

Syntax

```
enable authentication [local | remote | hint_assigned |
send_auth_service_type]
```

Table 162 Enable Authentication Parameters

Parameter	Description
local	User authentication based on a password specified in the User Table. When you issue the <code>add user</code> command, entering a password activates local authentication. If no password is specified (passwords are optional), and remote authentication is not enabled, the user is not able to establish a connection. Local authentication is enabled globally by default.
remote	Authentication based on a password specified in a RADIUS or TACACS+ server.
hint_assigned	Remote authentication employing <i>optional IP address</i> assignment. The router card automatically assigns a temporary IP address to every dial-in user and reports it with the Framed-IP-Address in the RADIUS authentication request record. The RADIUS server may choose to accept this IP address with an Authentication-Ack message or choose to assign another IP address with an Authentication-Ack message containing no Frame-IP-Address field. The default is disabled.
send_auth_service_type	Enables the sending of the service type to the RADIUS server. The default is enabled.



Local authentication takes precedence over remote authentication.

Related Commands

[disable authentication](#)

[set authentication](#)

set authentication This command configures remote (RADIUS) authentication for up to three servers.

The servers must be assigned a preference. For each authentication, the server with the highest preference will be tried first. Keep-alive messages poll the RADIUS servers continuously (the router card RADIUS Service-Loss-Busyout feature) to check if the servers are available. If the highest preference server is not available, then the next preferred server is tried. When a higher preference server is detected to be available again, then that server is used for authentication.

During the time retries are being sent to the next preferred server, if a higher preference server becomes available, then the retries to the current server are completed before switching to the higher preference server.

Syntax

```
set authentication
    per_server_retry_count <1 to 30>
    primary_destination_port <port number>
    primary_preference <1 to 3>
```

```

primary_secret <string>
primary_server <IP address or name>
retransmissions <count>
secondary_destination_port <port number>
secondary_preference <1 to 3>
secondary_secret <string>
secondary_server <IP address or name>
source_port <port number>
syslog_counters [disabled | enabled]
syslog_interval [five_days|one_day|one_hr|six_hr |twelve_hr]
syslog_reset [disabled | enabled]
tertiary_preference <1 to 3>
tertiary_destination_port <port number>
tertiary_secret <string>
tertiary_server <IP address or name>
timeout <period>
vsa [enabled | disabled]

```

Table 163 Set Authentication Command Parameters Descriptions

Parameter	Description	Settings	Default
per_server_retry_count	When authenticating a user, this is the number of times each configured server is tried in a round-robin fashion before the next server is tried.	1 to 30	3
primary_destination_port	RADIUS destination port for the primary authentication server.	0 to 65535	1812
primary_preference	Server with the highest preference for authentication.	1 to 3	—
primary_secret	Password of the Primary RADIUS server. A null string is valid.	Up to 16 ASCII characters.	—
primary_server	IP address or name of the initial server to exchange authentication data with.	xxx.xxx.xxx.xxx	—
retransmissions	Maximum number of times to retransmit packets to one or both servers if transmissions fail. A value of 0 causes infinite retries. We recommend you do not set the value to 0.	0 to 100	10
secondary_destination_port	RADIUS destination port for the secondary authentication server.	0 to 65535	1812
secondary_preference	Server with the second highest preference for authentication.	1 to 3	—
secondary_secret	Password of the Secondary RADIUS server. Null string as valid.	Up to 16 ASCII characters.	—

Table 163 Set Authentication Command Parameters Descriptions

Parameter	Description	Settings	Default
secondary_server	IP address or name of the second server to exchange authentication data with.	xxx.xxx.xxx.xxx	—
source_port	RADIUS source port for the primary authentication server.	0 to 65535	1812
syslog_counters	When enabled, counter values are sent to the syslogs configured in the system at regular intervals.	enable disable	—
syslog_interval	Determines the frequency in hours of syslogging.	five_days one_day one_hr six_hr twelve_hr	twelve_hr
syslog_reset	When enabled, the counters are reset each time after sending the current counter values to the syslogs. When disabled, the counters are cumulative.	enabled disabled	disabled

Related Commands

[show authentication settings](#)

show authentication settings

This command displays the RADIUS and local user authentication settings. Use [set authentication](#) to modify authentication settings.

Syntax

```
show authentication settings
```

The following information is listed:

- Local Authentication is—enabled (*default*)/disabled
- Remote Authentication is—enabled (*default*)/disabled
- Hint Assigned is—Whether IP address is assigned optionally by remote server. enabled/disabled (*default*)
- Primary Server is—IP address of the primary RADIUS server
- Primary Destination Port is—Port number of the primary server. The default is 1645.
- Secondary Server is—IP address of the secondary RADIUS server
- Secondary Destination Port is—Port number of the secondary server. The default is 1645.
- Tertiary Server is—IP address of the secondary RADIUS server
- Tertiary Destination Port is—Port number of the secondary server. The default is 1812.

- Source Port is—Port number of the source server. The default is 1812.
- Retransmission Timeout—Interval between retransmissions. The default is 3 seconds.
- Max Retranmissions—Number of retransmissions before failure reported. The default is 10 seconds.
- Per Server Retry Count—Number of retransmissions per server.
- Vendor Specific Attribute—Send vendor specific attribute.
- Prioritize Auth Server—In round-robin mode, tries the first server initially.
- Active Authentication Server—The server currently in use for authentication.
- Send service type indication—Enable or disable sending an indication of the service type.
- Authentication Counters Syslogs—Enable or disable authentication counters syslog.
- Authentication Counters Syslog Frequency—Frequency in hours the syslog counter is reset to zero (if Auth Counters Syslog Reset is enabled).
- Authentication Counters Syslog Reset—Enable or disable resetting counters at a configured interval (Auth Counters Syslog Frequency).
- Primary Auth Server Preference—Primary auth server preference value when using the preferred algorithm.
- Secondary Auth Server Preference—The secondary auth server preference value when using the preferred algorithm.
- Tertiary Auth Server Preference—The tertiary auth server preference value when using the preferred algorithm.

Example

```
show authentication settings
```

Related Commands

[set authentication](#)

CBCP Commands

The section covers commands to enable and disable Call Back Control Protocol (CBCP) using the CLI.

**enable ppp
negotiated_callback**

This command enables the negotiation of callback protocols in LCP phase of PPP. Callback control protocol (CBCP) is one such protocol negotiated.

This feature is disabled by default.

Syntax

```
enable ppp negotiated_callback
```

Example

```
enable ppp negotiated_callback
```

Related Commands

[disable ppp negotiated_callback](#)

**disable ppp
negotiated_callback**

Disables the negotiation of callback protocols in LCP phase of PPP. Callback control protocol (CBCP) is one such protocol negotiated.

This feature is disabled by default.

Syntax

```
disable ppp negotiated_callback
```

Example

```
disable ppp negotiated_callback
```

Related Commands

[enable ppp negotiated_callback](#)

IPsec (Policy) Commands

This section covers commands to add and remove IP security policy files using the CLI.

add policy This command adds an IPsec policy file into the system cache.

Syntax

```
add policy <filter name> print_access [on | off]
```

Table 164 Add Policy Command Parameters Descriptions

Parameter	Description	Settings
filter name	The name of the file which contains the IPsec filter policy.	Up to 20 ASCII characters
print_access	Turns on and off display of the compiled policy. The default is off.	on off



The Win 2000 Beta version does not support TUNNEL in Phase 2 of the IPSEC policy.

Example

```
add policy ipsecfile print_access on
```

Related Commands

[delete_policy](#)

delete policy This command removes the specified IPsec policy from the system cache configured with the [add_policy](#) command.

Syntax

```
delete policy <filter name>
```



If a policy failed to compile, it is automatically deleted and does not need to be manually deleted with this command.

Example

```
delete policy ipsecfile
```

Related Commands

[add_policy](#)

IPsec (IP Security) Commands

This section covers commands to control IP security options using the CLI.

enable ip security_option

This command allows global filtering of all IP packets containing the specified datagram fields. This security feature also syslogs the event when the packet is dropped. Refer to the [show packet logging](#) command for accounting data.

Syntax

```
enable ip security_option
    drop_all_fragoffset1
    drop_tcp_fragoffset1
    disallow_all_header_options
    disallow_source_route_options
```



Disallow and drop commands work in conjunction with each other. The `disallow_source_route_options` command is a subset of the `disallow_all_header_options` command. If you enable the source route command you must disable the all header command. But, enabling the more inclusive all header value renders the source route command unnecessary whether enabled or not. The same logic applies for drop commands.

The datagram fields shown below, when found, cause the packet to be dropped.

- fragment offset=1—Packets with an offset equal to one are discarded in accordance with RFC 1858. Some routers that may be used on the same network with the router card may be configured to filter out specific traffic. In some cases these routers will not apply the filter correctly for IP packets with an offset of 1. To avoid this hole in the filtering mechanism, packets of this type can be discarded. Of the two drop commands, this is the highest level of security. The default is enabled.
- partial TCP headers (offset=1)—Protocol field in the IP packet header (in this case, TCP). Packets of this type can be discarded. Lower level of security than All fragmented packets (Drop_all_fragoffset1). The default is enabled.
- all header options—All choices in the IP Options field of the IP header. IP options may be generated as an attack to get past routing tables. To avoid this hole in security, packets of this type can be discarded. Of the two disallow commands, this is the highest level of security. The default is disabled.
- source route options—Another choice in the IP Options field of the IP header. Particular path the sender chooses to take through the network to reach its destination, as specified in the sender packet's IP header. Packets of this type can be discarded although this is a lower level of security than All Header Options. The default is disabled.

Related Commands[show_packet_logging](#)[drop_all_fragoffset1](#)[show_ip_security_settings](#)**show ip security settings**

This command displays the status of IP security settings.

- Drop All Fragoffset1
- Drop TCP Fragoffset1
- Disallow All Header Options
- Disallow Source Route Options

Syntax

```
show ip security settings
```

Example

```
show ip security settings
```

Related Commands[enable_ip_security_option](#)**show security_option**

This command displays status of SNMP user access, security service and administration by remote users. Modify SNMP user access using the enable or disable security_option snmp commands. You can modify administration by remote user using the enable or disable security_option remote_user commands.

Syntax

```
show security_option settings
```

- **SNMP User Access**—enabled (default) or disabled
- **Security Service**—RADIUS or TACACS+
- **Administration by Remote Dialin User**—on (default) or off
- **Administration by Remote TELNET user**—on (default) or off

Example

```
show security_option settings
```

Related Commands

[disable security_option remote_user_administration](#)

[enable security_option remote_user_administration](#)

[enable security_option snmp_user_access](#)

disable ip security option

This set of commands disables the global filtering of all IP packets containing the specified datagram fields. This security feature also syslogs the event when the particular packet is dropped.

Syntax

```
disable ip security option  
    drop_all_fragoffset1  
    drop_tcp_fragoffset1  
    disallow_all_header_options  
    disallow_source_route_options
```

Example

```
disable ip security option drop_all_fragoffset1  
disable ip security option disallow_all_header_options
```

Related Commands

[enable ip security_option](#)

[show ip security settings](#)

Microsoft Point to Point Encryption Commands

For information on Microsoft Point to Point Encryption Commands MPPE see [set network user <user name> ppp encryption_algorithm](#).

Network Address Translation Commands

This section covers commands that address Network Address Translation (NAT) settings.

list nat sessions This command displays the following session information for NAT connections:

- Client_IP
- Peer_IP
- Trans_IP
- CPort
- PPort
- TPort
- Dir
- Time

Syntax

```
list nat sessions
```

Example

```
list nat sessions
```

Related Commands

[list nat stats](#)

list nat stats This command displays the following statistical information for NAT connections:

Counter for outgoing sessions

- Total Successfully created sessions
- Total Failed sessions
- Total Translated incoming packets
- Total Discarded incoming packets
- Total Translated outgoing packets
- Total Discarded outgoing packets

Counter for incoming sessions

- Total Successfully created sessions
- Total Failed sessions
- Total Translated incoming packets
- Total Discarded incoming packets
- Total Translated outgoing packets
- Total Discarded outgoing packets

Packet Filtering Commands

This section covers packet filtering and logging commands of the CLI.

add filter This command adds a filter file name to the Filter Table. The Filter Table is a managed list of filter names used by SNMP. A filter file is a text file stored in the Flash file system that you load from an external source using TFTP or create internally with the edit command. Add filter also verifies the syntax of the filter file. If syntax verification fails, you'll receive an error message, and the filter will still be added to the table, but is not usable. You must correct the filter file in a text editor, use TFTP to export the updated file to the system's FLASH file system, and use the [verify filter](#) command to check the filter's syntax. You can view the filters using the [show filter](#) command and verify whether the filter is correct by using the show file command.



Filter files are stored as ASCII files in Flash memory.



If a filter file is specified without an extension, the router card assumes RADIUS input filter files have the extension .in and that RADIUS output filter files have the extension .out. For this reason, RADIUS filter files should be named filter.in and filter.out.

Syntax

```
add filter <filter name>
```

Example

```
add filter secfilter2
```

Related Commands

[delete filter](#)

[list filters](#)

[show filter](#)

[verify filter](#)

delete filter This command removes the named filter from the Filter Table, and deletes the file stored in Flash memory. Use [list filters](#) to see filter files stored in FLASH memory.

Syntax

```
delete filter <filter name>
```

Example

```
delete filter secfilter2
```

Related Commands

[add filter](#)

[show filter](#)

[verify filter](#)

[list filters](#)

list filters This command displays all the filter names in the Filter Table, which you previously defined using the [add filter](#) command. You can remove filters using [delete filter](#).

Syntax

```
list filters
```

Table 165 List Filter Command Description

Parameter	Description
Filter Name	The filter file name.
Status	Current status of the filter. Choices are: Save—Filter file directed to be written to the current configuration file Saving—Filter file is being written to the new configuration file Normal—Filter file has been written to the configuration file Verify Failed—Filter verification failed
Protocols	Filter protocols supported. They are IP, IP-RIP, IP-CALL, IPX, IPX-CALL, IPX-SAP, IPX-RIP, LOGIN-ACCESS

Example

```
list filters
```

Related Commands

[add filter](#)

[delete filter](#)

[show filter](#)

[verify filter](#)

set interface This command sets filter parameters for the specified filter on the specified interface. You can see the available filter files using [list filters](#), view the contents of a filter file using [show filter](#), and add filter files to Flash memory using TFTP.



If a filter file is specified without an extension, the router card assumes RADIUS input filter files have the extension .in and that RADIUS output filter files have the extension .out. For this reason, RADIUS filter files should be named filter.in and filter.out.



Interface filters can be changed on-the-fly without disabling and re-enabling each network on that interface.

Syntax

```
set interface <interface name>
    filter_access [on | off]
    input_filter <filter name>
    output_filter <filter name>
    policy_access [private | public]
    policy_file <filter name>
```

Table 166 Set Interface Parameter Description

Parameter	Description	Settings
<interface name>	Designation of interface you are setting parameters for.	Up to 64 ASCII characters.
filter_access	Off causes filters specified for an interface with a set interface command to override filters specified with a set user command when the filters are of the same type. The default is Off.	on off
input_filter	Name of the filter file you wish to be applied to the input stream coming in on the specified interface.	Up to 20 ASCII characters.
output_filter	Name of the filter file you wish to be applied to the output stream leaving the specified interface.	Up to 20 ASCII characters.
policy_access	Specifies whether an interface is public or private. A public interface is an interface that is directly connected to a public network or Internet. A private interface is an interface that is directly connected to a private network.	private public
policy_file	Configures a policy on an interface. For example: set interface eth:1 policy_file "r&dpolicy" A policy can also be attached to the internal device. This would be efficient for the internal applications like L2TP, PPTP, SNMP etc.	—

Related Commands

[disable interface](#)

[enable interface](#)

[list interfaces](#)

[show icmp settings](#)

[show interface <interface name> settings](#)

set packet_logging

This command sets parameters to generate SYSLOG messages for filtered packets. Facility can be configured *globally*, for specific users who have the Log-Filter-Packet attribute set in the Access-Accept RADIUS configuration, or not at all. Use the [show packet_logging](#) command to view settings.

Syntax

```
set packet_logging
    logging [all | none | radius]
    packet_size [0 to 493 bytes]
```

Table 167 Set Packet_Logging Command Parameter Descriptions

Parameter	Description	Settings	Default
logging	Specifies type of logging generated.	All—all filtered packets generate a SYSLOG message RADIUS—the RADIUS attribute, Filter-Log-Packet, to control SYSLOG message generation for a specified user None—no SYSLOG messages are generated.	None
packet_size	Specifies the size of a filtered packet that will be included in the actual SYSLOG message. When set to zero (0), the size feature is turned off, causing the entire packet to be included in the SYSLOG message.	0 to 493 bytes	0

Example

```
set packet_logging logging all packet_size 256
```

show filter This command displays the filter rules for all protocols specified in this file. The file name specified must be a filter file (*filter.fil*). Also, see the edit command to create or amend filter files.



A newly created filter file will not appear when this command is issued until the file is added to the Filter Table with the [add filter](#) command.

Syntax

```
show filter <filter name>

        protocol [ip, ip-call, ip-rip, ipx, ipx-call, ipx-rip,
        ipx-sap, login-access]
```

The protocol parameter displays filter rules based on the protocol options specified. The filter name must be a filter file (*filter.fil*), as listed using the [list filters](#) command. The values for the protocol parameter are as follows:

- ip—IP data filter rules
- ip-call—IP call filter rules
- ip-rip—IP RIP advertisement filter rules
- ipx—IPX data filter rules
- ipx-call—IPX call filter rules
- ipx-rip—IPX RIP advertisement filter rules
- ipx-sap—IPX SAP advertisement filter rules
- login-access—Login access filter rules

Example

The following is an example of output from the show filter command:

```
RULES FOR FILTER ./easyfilter.fil SHOW PROTOCOLS: ALL
#filter
IP:
10 REJECT src-addr = 234.149. 82.139;
20 ACCEPT src-addr != 234.149. 82.139;
30 REJECT udp-src-port = 69;
40 REJECT tcp-src-port = 23;
50 REJECT udp-dst-port = 69;
60 REJECT tcp-dst-port = 23;
IP-RIP:
10 ACCEPT network = 244.49.82.0;
20 deny
```

Related Commands

[add filter](#)
[delete filter](#)
[list filters](#)
[verify filter](#)

verify filter This command verifies the syntax of a filter file, which has been previously added to the table. If you update a filter file and TFTP it to the Flash file system, and the file already exists in the Filter Table, use this command to verify the files syntax. Use the [list filters](#) command to see which files are currently in the Filter File Table, and the status of each.

Syntax

```
verify filter <filter name>
```

Example

```
verify filter easyfilter.fil
```

Related Commands

[add filter](#)
[delete filter](#)
[show filter](#)
[list filters](#)

set policy update This command updates a policy that was already loaded into the system. The updated policy is used only for new connections and does not affect existing connections. The parameter filter_name is the name of policy file to use when updating the IPsec policy in the system cache.



The Win 2000 Beta version does not support TUNNEL in Phase 2 of the IPSEC policy.



When using Cisco2500 as a gateway, for IPSEC policy file use Preshared Key length up to 63 characters as it only allows 63 characters for IPSEC SA to be established successfully.

Syntax

```
set policy update <filter name>
```

Example

```
set policy update filter3.fil
```

RADIUS

This section covers Remote Authentication Dial-in User Service (RADIUS) commands of the CLI.

set accounting This command configures RADIUS accounting. Use the [show accounting](#) command to check these values.

The router card has two server groups (Primary & Secondary) each comprising one main server and two backup servers. Accounting may be enabled independently for the two groups. Within each group, a round-robin strategy is followed. Each of the three servers in a group is tried once until max retries have been reached. For example, in the primary group if the main server A1 and the backup servers are A2 & A3, the sequence of tries is A1, A2, A3, A1, A2, A3 and so on until accounting is successful or the total number of retries N has been reached. The first server to be tried is always A1.



The IP address/port number pair for accounting and backup servers must be unique or conflicts will occur. In other words, one accounting server designated as both first and second server must have unique port numbers designated for both servers. The same port number can be designated on servers with different IP addresses, though.

Syntax

```
set accounting
  attribute_style [netserver | standard]
  log_unauthenticated_calls [enable | disable]
  primary_destination_port <port number>
  enhanced_tunneling_accounting [enable | disable]
  a1 destination_port <port number>
  primary_retransmissions <number>
  primary_secret <"secret string">
  a1 secret <"secret string">
  primary_server <IP address or host name>
  a1 address <IP address or host name>
  secondary_destination_port <port number>
  secondary_retransmissions <number>
  secondary_secret <"secret string">
  secondary_server <IP address or host name>
  b1 address <IP address or host name>
  source_port <port number>
  start_time [authentication | connection]
  timeout <number seconds>
  vsa [enabled | disabled]
  per_server_retransmissions <0 to 30>
```

```

syslog_counters [disabled | enabled]
syslog_interval [five_days|one_day|one_hr|six_hr|twelve_hr]
syslog_reset [disabled | enabled]
vtp_tunnel_flag [disabled | enabled]

```

Table 168 Set Accounting Parameter Commands

Parameter	Description	Settings	Default
attribute_style	Sets Unauthenticated Time (RADIUS attribute #9012) value. If set to netserver, unauthenticated time is the interval from when the call arrived to when the Access-Accept message is received; to set to standard, unauthenticated time is the interval from when the call was connected to when the Access-Accept message is received.	netserver standard	
log_unauthenticated_calls	Sets the router card to log calls which fail prior to authentication.	enabled disabled	enable
primary_destination_port a1 destination_port	Destination port number of the primary RADIUS server. To ensure correct identification of server response packets, configure a unique IP address/port combination.	0 to 65535	1813
enhanced_tunneling_ accounting	Provides features of advanced tunneling for use with accounting.	enabled disabled	—
primary_retransmissions	The interval the router card waits for a response from the primary server before retransmitting. A value of 0 causes infinite retransmissions. We recommend you do not set to 0.	0 to 2147483647	—
primary_secret a1 secret	Password of the Primary RADIUS server. The null string is supported.	Up to 16 ASCII characters.	—
primary_server a1 address	Initial server to send the accounting information to. To ensure correct identification of server response packets, configure a unique IP address/port combination.	xxx.xxx.xxx.xxx or host name	—

Table 168 Set Accounting Parameter Commands

Parameter	Description	Settings	Default
secondary_destination_port b1 destination_port	Destination port number of the Secondary RADIUS server. To ensure correct identification of server response packets, configure a unique IP address/port combination.	0 to 65535	1813
secondary_retransmissions	The interval the router card waits for a response from the secondary server before retransmitting. A value of 0 causes infinite retransmissions.	0 to 2147483647	—
secondary_secret b1 secret	Password of the Secondary RADIUS server. The null string is supported.	Up to 16 ASCII characters	—
secondary_server b1 address	Second server to send the accounting information to. To ensure correct identification of server response packets, configure a unique IP address/port combination.	xxx.xxx.xxx.xxx or host name	—
source_port	Port number of the source port of the primary accounting server.	0 to 65535	1813
start_time	The point at which accounting begins. authentication—session time in number of seconds after user name and password are entered. connection—session time in number of seconds from modem pickup.	authentication connection	—
timeout	Interval between retransmissions.	1 to 60	5
vsa	Enables/disables transmission of Vendor Specific Attributes to specified RADIUS servers.	enabled disabled	—
per_server_retransmissions	When authenticating a user, this is the number of retransmissions each configured server is tried in a round-robin fashion before the next server is tried. Default value is 3 .	0 to 30	3
syslog_counters	When enabled, counter values are sent to the syslogs configured in the system at regular intervals.	enabled disabled	—

Table 168 Set Accounting Parameter Commands

Parameter	Description	Settings	Default
syslog_interval	Determines the frequency of syslogging.	five_days one_day one_hr six_hr twelve_hr	twelve_hr
syslog_reset	When enabled, the counters are reset each time after sending the current counter values to the syslogs. When disabled, the counters are cumulative.	enabled disabled	disabled
vtp_tunnel_flag	When enabled, in the case of MPIP, the tunneled link will send an accounting request from both the MPIP tunnel initiator and the MPIP tunnel terminator. When disabled, no accounting request is sent.	enabled disabled	—

Related Commands

[disable_secondary_accounting_server](#)

[enable_prioritize_first_accounting_server_in_a_group](#)

[show_accounting](#)

set accounting_backup primary

This command configures first and second backup servers for the primary accounting server group. The router card delivers accounting packets to primary *and* secondary server groups independently so that if all servers in one server group are not responsive, packets will be received successfully by the other group. Further redundancy is insured by having a first and second backup server per server group. If a server within a server group does not respond when a packet is transmitted to it, the packet is retransmitted to the next backup server in *round-robin* fashion.



The IP address/port number pair for accounting and backup servers must be unique or conflicts will occur. In other words, one accounting server designated as both first and second server must have unique port numbers designated for both servers. The same port number can be designated on servers with different IP addresses, though.

Syntax

```
set accounting_backup primary
    first_destination_port <port>
    a2 destination_port <port>
    first_secret <string>
```

```

a2 secret <string>
first_server <IP address or host name>
a2 address <IP address or host name>
second_destination_port <port>
a3 destination_port
second_secret <string>
a3 secret <string>
second_server <IP address or host name>
a3 address <IP address or host name>

```

Table 169 Set Accounting Backup Primary Commands

Parameter	Description	Settings	Default
first_destination_port a2 destination_port	RADIUS destination port number of the first backup server for the primary server group. To ensure correct identification of server response packets, configure a unique IP address/port combination.	0 to 65535	1813
first_secret a2 secret	Password of the first backup server for the primary accounting server group. Null string: ""	Up to 16 ASCII characters.	—
first_server a2 address	Unique designation for initial backup server in the primary accounting server group. To ensure correct identification of server response packets, configure a unique IP address/port combination.	xxx.xxx.xxx.xxx	—
second_destination_port a3 destination_port	RADIUS destination port number of the second backup server for the primary accounting server group. To ensure correct identification of server response packets, configure a unique IP address/port combination.	0 to 65535	1813
second_secret a3 secret	Password of the secondary RADIUS server for the primary accounting server group. Null string: ""	Up to 16 ASCII characters.	—
second_server a3 address	Unique designation for second backup server in the primary accounting server group. To ensure correct identification of server response packets, configure a <i>unique</i> IP address/port combination.	xxx.xxx.xxx.xxx	—

Related Commands

[disable_secondary_accounting_server](#)

[enable_prioritize_first_accounting_server_in_a_group](#)

[enable_secondary_accounting_server](#)

[set_accounting_backup_secondary](#)

**set accounting_backup
secondary**

This command configures first and second backup servers for the secondary accounting server group. The router card delivers accounting packets to primary *and* secondary server groups independently so that if all servers in one server group are not responsive, packets will be received successfully by the other group. Further redundancy is insured by having a first and second backup server per server group. If a server within a server group does not respond when a packet is transmitted to it, the packet is retransmitted to the next backup server in round-robin fashion.



The IP address/port number pair for accounting and backup servers must be unique or conflicts will occur. In other words, one accounting server designated as both first and second server must have unique port numbers designated for both servers. The same port number can be designated on servers with different IP addresses, though.

Use the enable and disable primary_accounting_server and secondary_accounting_server commands to control this feature.

Syntax

```
set accounting_backup secondary
    first_destination_port <port>
    b2 destination_port <port>
    first_secret <string>
    b2 secret <string>
    first_server <IP address or host name>
    b2 address <IP address or host name>
    second_destination_port <port>
    b3 destination_port <port>
    second_secret <string>
    b3 secret <string>
    second_server <IP address or host name>
    b3 address <IP address or host name>
```

Table 170 Set Accounting Backup Secondary Commands

Parameter	Description	Settings	Default
first_destination_port b2 destination_port	RADIUS destination port number of the first backup server for the secondary accounting server group. To ensure correct identification of server response packets, configure a unique IP address/port combination.	0 to 65535	1813
first_secret b2 secret	Password of the first backup server for the secondary accounting server group. Null string: ""	Up to 16 ASCII characters.	—
first_server b2 address	Unique designation for initial backup server in the secondary accounting server group. To ensure correct identification of server response packets, configure a unique IP address/port combination.	xxx.xxx.xxx.xxx or host name	—
second_destination_port b3 destination_port	RADIUS destination port number of the second backup server for the secondary accounting server group. To ensure correct identification of server response packets, configure a unique IP address/port combination.	0 to 65535	1813
second_secret b3 secret	Password of the secondary RADIUS server for the secondary accounting server group. Null string: ""	Up to 16 ASCII characters.	—
second_server b3 address	Unique designation for second backup server in the secondary accounting server group. To ensure correct identification of server response packets, configure a unique IP address/port combination.	xxx.xxx.xxx.xxx or host name	—

Related Commands[disable_secondary_accounting_server](#)[enable_prioritize_first_accounting_server_in_a_group](#)[enable_secondary_accounting_server](#)[set_accounting_backup_primary](#)

**set accounting
call_detail_record
[disabled | enabled]**

When enabled, this feature provides additional vendor-specific attributes (VSAs) to the contents of each RADIUS accounting stop message generated by the router card.

A modem call record contains attributes logically grouped into six categories as in the following:

Group 1 Attributes—Usage Statistics

- User Name
- Call Start Date/Time
- Call End Date/Time
- Call Termination Reason
- ANI (**inbound only)
- DNIS (**inbound only)
- Number Dialed (**outgoing only)
- Call Duration

Group 2 Attributes—Data Transfer Statistics

- Characters Send
- Characters Received
- Octets Sent
- Octets Received
- Block Sent
- Blocks Received
- Characters Lost
- Line Reversals

Group 3—Performance Statistics

- Block CRC Errors
- Link NAKs
- Link Fallbacks
- Link Upshifts
- Initial Link TX Rate
- Final Link TX Rate
- Initial Link RX Rate
- Final Link RX Rate
- Retrans Requested
- Retrans Granted

Group 4—Operating Mode Statistics

- Sync/Async Mode
- Modulation Type
- Originate / Answer Mode
- Error Control Type
- Data Compression Type
- HST Back Channel Rate
- Default DTE Data Rate
- High Freq. Equalization
- On-Line Fallback

Group 5—Remote Modem Management Information Exchange

- Manufacturer ID
- Product Code
- Serial Number
- Firmware Version
- Firmware Build Date
- RMME Status
- RMMIE Number of Updates
- X2 Status
- Planned Disconnect Reason

Group 6—VOIP Specific Statistics

- Packets Sent
- Packets Received
- Packet Lost

**set accounting
server_group [a | b]
retransmissions**

This command sets the number of retransmissions of the reboot message sent by the router card to each configured server in a round-robin fashion with the most preferred server being tried first. If no reply is received, the server must be tried M times before switching to the next server where M is the number of retries per server. It is sufficient if any server replies to this message.

Syntax

```
set accounting server_group [a | b] retransmissions <0 to
2147483647>
```

Example

```
set accounting server_group b retransmissions 1000
```

**set acct_format [all |
simple | sprint]**

This command configures different attribute formats for accounting.

Syntax

```
set acct_format [all | simple | sprint]
```

Table 171 Set Acct_format Descriptions

Parameter	Description
all	Accounting attributes that the router card can provide
simple	Attributes format based on the Sprint CRD and CP Version 1.2 in with TACACS+. Default.
sprint	Vendor-specific attributes format based on Sprint specifications

Example

```
set acct_format sprint
```

set radius This command sets RADIUS authentication parameters including the descriptive *style* of attributes you prefer to use, the *authentication* procedure employed and the *interval* between accounting packet transmission.

The `authentication_algorithm` parameter works in the following manner. The router cardrouter card refers to its Authentication Table for the IP addresses of RADIUS servers when RADIUS requests are received. When no response is received from the primary server within a specified interval, the RADIUS request is re-transmitted to the primary *and* secondary servers via a *fall-through* algorithm. Another available selection process shares the authentication load using a *round_robin* algorithm to query the primary, secondary or tertiary servers until an authentication response is received. This is done by the router card's Authentication Table which keeps track of the last server tried successfully, making the next authentication request to the previously successful server first. If during this cycle the maximum retransmission value is reached, authentication requests are terminated. You may configure this value using the [set authentication](#) command. The default is **round_robin**.

Setting the *interim accounting interval* specifies how often checkpoint accounting packets are sent to the accounting server.

Syntax

```
set radius
    attribute_style [standard | ascend | mci]
    authentication_algorithm [fall_through|round_robin|
    active_server|preferred]
    dnis_auth_service_type [0, 255]
    dnis_nas_port_style [default, null]
    interim_accounting_interval [5, 3600]
    port_id_style [continuous | density_based]
    resource_reclaim_style [draft | mci]
    reboot_indication_style [fall_through | preferred_server]
    nas_port_format [default | format_one | standard]
    auth_service_type [0 to 255]
```

Table 172 Set RADIUS Command Parameters Descriptions

Parameter	Description	Settings
attribute_style	Method used to describe RADIUS attributes.	standard ascend mci
authentication_algorithm	Algorithm type to be used in selecting a RADIUS authentication server from those servers available:	fall-through round_robin active_server preferred
dnis_auth_service_type	The service type sent for DNIS authentication. Standard RADIUS authentication expects a service type of 10. The default is 10.	0 to 255
dnis_nas_port_style	The NAS port style used for accounting.	default null
interim_accounting_interval	Interval in seconds between interim accounting packet transmissions by the router card.	5 to 3600
port_id_style	<p>The continuous style generates the port id sequentially starting from 1. This allows the router card to maintain a table of port-ids ranging from 1 to the maximum number of calls that can be handled by the chassis. For each call, the smallest available number in a table is assigned as the port id for the call. An internal mapping of slot & channel numbers to the assigned port-id is kept by the router card. The Start, Stop and Interim accounting packets for a call will bear this assigned port-id. This method ensures that the port ids seen by the RADIUS server will fall within the desired range without any holes.</p> <p>This method works irrespective of cards being removed, added or swapped in the chassis, since the port-ids are assigned on the fly. If the RADIUS server does require the Slot and Channel values, they can be obtained from the RADIUS attributes that are contained in each packet sent by the router card.</p> <p>The density-based style of generating the port id uses the formula: (slot# * reported_port_density) + channel# + port_base. The default value for reported_port_density is 256 and the port_base is 1. Since the reported_port_density is 256, there are potential holes in the range of port ids that are generated by the router card.</p> <p>The default is density_based.</p>	continuous density_based

Table 172 Set RADIUS Command Parameters Descriptions

Parameter	Description	Settings
resource_reclaim_style	<p>If you select draft for the resource_reclaim style, the resource-reclaim message from the RADIUS server has the port-id and optionally the username attributes. The user session corresponding to the port-id is looked up for disconnecting. If the username attribute is absent in the reclaim message, the user session is simply disconnected. If the username is present in the message, it is compared with the corresponding parameter in the user session. If there is a match, the user session is disconnected; if there is no match, the message is discarded.</p> <p>The mci resource reclaim style works as follows: If the username is present in the reclaim message and if the port-id attribute has value zero, then all user sessions corresponding to that username must be disconnected.</p>	<p>draft</p> <p>mci</p>
reboot_indication_style	<p>Whether reboot indication is sent in fall-through fashion or in round-robin manner according to server preference. The default is fall-through.</p>	<p>fall_through</p> <p>preferred_server</p>
nas_port_format	<p>Indicates the format the information will be represented in the RADIUS packet. The default is default.</p>	<p>default</p> <p>format_one</p> <p>standard</p>
auth_service_type	Indicates the service type used for RADIUS information.	0 to 255

set security_service This command generates RADIUS or TACACS+ service upon the router card bootup. Configuring this service to *tacacsplus* enables EAP support. The default is RADIUS.

Syntax

```
set security_service [radius | tacacsplus]
```

Example

```
set security_service tacacsplus
```

set service_loss_busyout radius frequency This command sets the interval at which network connectivity will be checked by a RADIUS server. If service is lost to the RADIUS server after a specified period (*frequency*), the router card will busy out the Hub's modems. The router card will continuously poll the RADIUS server until connectivity is restored and, at that point, restore the Hub's modem's to their normal state. The default is 60 seconds. The range is 1 to 200 seconds.

Syntax

```
set service_loss_busyout radius frequency <interval>
```

Example

```
set service_loss_busyout radius frequency 100
```

Accounting Server Commands

This section covers accounting server commands of the CLI.

disable primary_accounting_server This command disables the primary accounting server. Refer to the command to configure the primary accounting server.

Syntax

```
disable primary_accounting_server
```

Example

```
disable primary_accounting_server
```

Related Commands

[enable prioritize_first_accounting_server_in_a_group](#)

[set accounting](#)

[show accounting](#)

**enable
primary_accounting_
server**

This command enables the primary accounting server configured with the [set accounting](#) command.

Syntax

```
enable primary_accounting_server
```

Example

```
enable primary_accounting_server
```

Related Commands

[disable secondary_accounting_server](#)

[set accounting](#)

[show accounting](#)

**enable prioritize_first_
accounting_server_in_
a_group**

When the first accounting server is unavailable, the accounting packets are sent to the backup accounting servers. When the primary accounting server comes back up accounting packets will again be sent to it first. The default is Disabled.

Syntax

```
enable prioritize_first_accounting_server_in_a_group
```

Example

When the switch is on and when the primary server is down, the accounting packets are sent to the primary as well as the primary_first_back or primary_second_back servers (depending on the Round-Robin retries). In this case the accounting packets are always sent to the primary server.

Related Commands

[disable prioritize_first_accounting_server_in_a_group](#)

[show accounting](#)

**enable
secondary_accounting_
server**

This command enables the secondary accounting server. Configure the secondary accounting server with the [set accounting](#) command.

Syntax

```
enable secondary_accounting_server
```

Example

```
enable secondary_accounting_server
```

Related Commands

[disable secondary_accounting_server](#)

[set accounting](#)

[show accounting](#)

disable prioritize_first_accounting_server_in_a_group

This command disables prioritizing the first server in an accounting server-group. This is disabled by default.

Syntax

```
disable prioritize_first_accounting_server_in_a_group
```

Example

```
disable prioritize_first_accounting_server_in_a_group
```

Related Commands

[enable prioritize_first_accounting_server_in_a_group](#)

[show accounting](#)

disable secondary_accounting_server

This command disables the secondary accounting server.

Syntax

```
disable secondary_accounting_server
```

Example

```
disable secondary_accounting_server
```

Related Commands

[enable secondary_accounting_server](#)

[set accounting](#)

[show accounting](#)

show accounting

This command displays RADIUS accounting settings, which you can modify using the [set accounting](#) command.

Syntax

```
show accounting settings
```

- Primary Server Status—Current status of primary RADIUS server. The default is enabled.
- Primary Server—IP address of the primary RADIUS server.
- Primary First Backup Server—IP address of the primary RADIUS first backup server.
- Primary Second Backup Server—IP address of the primary RADIUS second backup server.
- Primary Destination Port—Destination port of the RADIUS primary server.
- Primary First Backup Destination Port—Destination port of the primary RADIUS first backup server.
- Primary Second Backup Destination Port—Destination port of the primary RADIUS second backup server.

- Max Primary Retransmissions—The number of times a packet is sent to the primary server group before the packet is discarded. The default is 0 which means infinite retries.
- Secondary Server Status—Current status of secondary RADIUS server. The default is enabled.
- Secondary Server—IP address of the secondary RADIUS server.
- Secondary First Backup Server—IP address of the secondary RADIUS first backup server.
- Secondary Second Backup Server—IP address of the secondary RADIUS second backup server.
- Secondary Destination Port—Destination port of the RADIUS secondary server.
- Secondary First Backup Destination Port—Destination port of the secondary RADIUS first backup server.
- Secondary Second Backup Destination Port—Destination port of the secondary RADIUS second backup server.
- Max Secondary Retransmissions—The number of times a packet is sent to the secondary server group before the packet is discarded. The default is 0 which means infinite retries.
- Source Port—RADIUS accounting port. The default is 1813.
- Retransmission Timeout—number of seconds between retransmissions. The default is 60.
- Per Server Retry Count—number of retransmissions per server.
- Accounting Start Time—the point at which accounting was begun by the enable accounting command.
- Log Unauthenticated Calls—current state of feature which logs calls failing prior to authentication. The default is *True*.
- Vendor Specific Attribute—send vendor specific attribute.
- Active Accounting Server (Primary)—primary server currently in use for accounting.
- Active Accounting Server (Secondary)—secondary server currently in use for accounting.
- Attribute Style—Shows the setting for Unauthenticated Time (RADIUS attribute #9012) value. If set to *netserver*, unauthenticated time is the interval from when the call arrived to when the Access-Accept message is received; to set to *standard*, unauthenticated time is the interval from when the call was connected to when the Access-Accept message is received.
- Prioritize First Server in a Server Group—when enabled and the first server is down the accounting packets go to the backup servers, it also tries to come back to the primary server if it comes back up.

Related Commands

[enable_prioritize_first_accounting_server_in_a_group](#)
[set_accounting](#)

show contact This command displays the settings (busyout enabled or disabled and busyout frequency in seconds) for the RADIUS busyout feature.

Syntax

```
show contact settings
```

Example

```
show contact settings
show contact
```

show contact timers This command displays the last time the router card heard from the different RADIUS accounting and authentication servers.

Syntax

```
show contact timers
```

Example

```
show contact timers
```

show radius This command displays current RADIUS accounting and authentication configuration.

Syntax

```
show radius settings
```

Example

```
show radius settings
```

show radius resource_management settings This command displays whether RADIUS resource management is enabled or disabled on the access router card.

Syntax

```
show radius resource_management settings
```

Example

```
show radius resource_management settings
```

Related Commands

[disable radius resource_management](#)

[enable radius resource_management](#)

[show radius resource_management counters](#)

show radius resource_management counters

This command displays resource management counters.

Syntax

```
show radius resource_management counters
```

Example

```
show radius resource_management counters
```

Related Commands

[disable radius resource_management](#)

[enable radius resource_management](#)

[show radius resource_management counters](#)

show service_loss_busyout settings

This command displays service loss busyout settings for RADIUS and ping, including frequency of busyouts and busyout status. Use [set service_loss_busyout radius frequency](#) and [add ping service_loss_system](#) to configure this RADIUS/PING function. Use [enable service_loss_busyout \[ping | radius\]](#) to enable RADIUS or PING busyout.

Syntax

```
show service_loss_busyout settings
```

Example

```
show service_loss_busyout settings
```

Related Commands

[set service_loss_busyout radius frequency](#)

[add ping service_loss_system](#)

[enable service_loss_busyout \[ping | radius\]](#)

disable accounting

This command disables remote accounting via RADIUS or TACACS+. Use [show accounting](#) to see if it is currently running.

Syntax

```
disable accounting
```

Example

```
disable accounting
```

Related Commands

[enable accounting](#)

disable accounting server_group

This command disables remote accounting via RADIUS or TACACS+ on the primary servers (a) or the secondary servers (b).

Syntax

```
disable accounting server_group [a | b]
```

Example

```
disable accounting server_group a
```

Related Commands

[enable accounting server_group \[a | b\]](#)

disable radius accounting

This command disables specified RADIUS accounting information.

Syntax

```
disable radius accounting  
    only_stop_for_failed_service  
    report_ip_only_for_primary_link  
    syslog_counters
```

Table 173 Disable Radius Accounting Command Parameters

Parameter	Description
only_stop_for_failed_service	Disables sending only a STOP ACCOUNTING record for a call when a PPTP/L2TP call setup fails after authentication but before establishment of the tunnel.
report_ip_only_for_primary_link	Disables sending 0.0.0.0 IP address for any non-primary link in the accounting records. This is disabled by default.
syslog_counters	Disables sending accounting statistics at regular intervals to the system logs configured in the system. Refer to set accounting syslog_interval .

Example

```
disable radius accounting syslog_counters
```

Related Commands

```
enable radius accounting  
show radius
```

**disable radius
fill_null_attributes**

This command disables the filling of *null* attributes in RADIUS accounting and authentication packets. Issue the [show radius settings](#) command to view settings.

Syntax

```
disable radius fill_null_attributes
```

Example

```
disable radius fill_null_attributes
```

Related Commands

[enable radius fill_null_attributes](#)

[show radius settings](#)

**disable radius
interim_accounting_
interval**

This command disables interim accounting on the RADIUS server configured with the [set radius](#) command. Issue the [show radius settings](#) command to view settings. The default is disabled.

Syntax

```
disable radius interim_accounting_interval
```

Example

```
disable radius interim_accounting_interval
```

Related Commands

[enable radius interim_accounting_interval](#)

[show radius settings](#)

**disable radius
resource_management**

This command disables resource management on the router card. When disabled, the router card:

- Does not send the NAS-Reboot-Indication and Resource-Free-Request messages.
- Sends Command-Unrecognized packets in response to Resource-Query-Request and Resource-Reclaim-Request packets sent from the RADIUS server.

Syntax

```
disable radius resource_management
```

Example

```
disable radius resource_management
```

Related Commands

[enable radius resource_management](#)

[show radius resource_management settings](#)

[show radius resource_management counters](#)

**disable radius
send_acct_for_default_
user**

This command disables the sending of accounting for users named “default”. This is enabled by default.

Syntax

```
disable radius send_acct_for_default_user
```

Example

```
disable radius send_acct_for_default_user
```

Related Commands

[enable radius send_acct_for_default_user](#)

[show radius settings](#)

**disable radius
source_port_
authentication**

This command disables checking that the source port in the RADIUS packets received from the RADIUS authentication server are the same as configured in the router card. The default is enabled.

Syntax

```
disable radius source_port_authentication
```

Example

```
disable radius source_port_authentication
```

Related Commands

[enable radius source_port_authentication](#)

[show radius settings](#)

**disable radius
use_radius_username**

This command disallows the User Name attribute in the RADIUS access_accept packet to override the default supplied in the request. Issue the [enable radius use_radius_username](#) command to turn this feature on. Use the [show radius settings](#) command to view the current value for this parameter. The default is disabled.

Syntax

```
disable radius use_radius_username
```

Example

```
disable radius use_radius_username
```

Related Commands

[enable radius use_radius_username](#)

[show radius settings](#)

**disable
service_loss_busyout
[ping | radius]**

This command disallows busying out of modems if there is no connectivity to the RADIUS or PING servers. Use the [show service_loss_busyout settings](#) command to view edits.



Both the PING and RADIUS busy out features cannot be enabled at the same time. If the PING busy-out feature is enabled and you attempt to enable RADIUS busy-out, you'll receive an error message.

Syntax

```
disable service_loss_busyout [ping | radius]
```

Example

```
disable service_loss_busyout radius
```

Related Commands

[enable service_loss_busyout \[ping | radius\]](#)

[show service_loss_busyout settings](#)

enable accounting

This command enables remote accounting via RADIUS or TACACS+. Use [show accounting](#) to determine if accounting is running.

Syntax

```
enable accounting
```

Example

```
enable accounting
```

Related Commands

[disable accounting](#)

[show accounting](#)

**enable accounting
server_group [a | b]**

This command enables remote accounting via RADIUS or TACACS+ on the primary servers (a) or the secondary servers (b).

Syntax

```
enable accounting server_group [a | b]
```

Example

```
enable accounting server_group b
```

Related Commands

[disable accounting server_group](#)

**enable radius
accounting**

This command enables RADIUS accounting settings.

Syntax

```
enable radius accounting
    only_stop_for_failed_service
    report_ip_only_for_primary_link
    syslog_counters
```

Table 174 Enable Radius Accounting Command Parameters Descriptions

Parameter	Description
only_stop_for_failed_service	Enables sending only a STOP ACCOUNTING record for a call when a PPTP/L2TP call setup fails after authentication but before establishment of the tunnel.
report_ip_only_for_primary_link	Enables sending 0.0.0.0 IP address for any non-primary link in the accounting records. This is disabled by default.
syslog_counters	Enables sending accounting statistics at regular intervals to the system logs configured in the system. Also refer to set accounting syslog_interval.

Example

```
enable radius accounting only_stop_for_failed_service
```

Related Commands

[disable radius accounting](#)

[show radius](#)

**enable radius
authentication
syslog_counters**

This command enables sending authentication statistics at regular intervals to the system logs configured in the system.

Syntax

```
enable radius authentication syslog_counters
```

Example

```
enable radius authentication syslog_counters
```

**enable radius
ignore_source_port**

This command enables verifying the source port of RADIUS packet received from the RADIUS server. By default, verification is enabled. The source port should be the same as the destination port in the RADIUS packet sent to the RADIUS Server.

Syntax

```
enable radius ignore_source_port
```

Example

```
enable radius ignore_source_port
```

**disable radius
ignore_source_port**

This command disables verifying the source port of RADIUS packet received from the RADIUS server.

Syntax

```
disable radius ignore_source_port
```

Example

```
disable radius ignore_source_port
```

**enable radius
send_unauth_
acct_record**

This command enables sending of accounting stop packets for calls failed before authentication. The username field will be unauthenticated in these accounting packets.

Syntax

```
enable radius send_unauth_acct_record
```

Example

```
enable radius send_unauth_acct_record
```

Related Commands

[disable radius fill_null_attributes](#)

[show radius settings](#)

**disable radius
send_unauth_
acct_record**

This command disables sending of accounting stop packets for calls failed before authentication.

Syntax

```
disable radius send_unauth_acct_record
```

Example

```
disable radius send_unauth_acct_record
```

Related Commands

[disable radius fill_null_attributes](#)

[show radius settings](#)

**enable radius
fill_null_attributes**

This command permits the filling of null attributes in RADIUS accounting and authentication packets. If enabled, RADIUS accounting/authentication records will contain attributes with 'X' rather than a null string.

Syntax

```
enable radius fill_null_attributes
```

Example

```
enable radius fill_null_attributes
```

Related Commands

[disable radius fill_null_attributes](#)

[show radius settings](#)

**enable radius
interim_accounting_
interval**

This command permits interim accounting on the RADIUS server configured with the [set radius](#) command. The default is disabled.

Syntax

```
enable radius interim_accounting_interval
```

Example

```
enable radius interim_accounting_interval
```

Related Commands

[disable radius interim_accounting_interval](#)

[show radius settings](#)

[set radius](#)

**enable radius
resource_management**

This command enables resource management on the router card. When enabled, the router card:

- Sends the NAS-Reboot-Indication upon reboot.
- Sends replies to the Resource-Query-Request messages sent from the RADIUS server.
- Sends a Resource-Free-Request message whenever a user disconnects (provided that the Terminate-Action attribute is set to 2 in the Access-Accept message for the user).
- Sends Command-Unrecognized messages in response to message types that are not supported.

Syntax

```
enable radius resource_management
```

Example

```
enable radius resource_management
```

Related Commands

[disable radius resource_management](#)

[show radius resource_management settings](#)

[show radius resource_management counters](#)

**enable radius
resource_free tunnel_
initiator**

This command enables the resource-free tunnel initiator.

Syntax

```
enable radius resource_free tunnel_initiator
```

Example

```
enable radius resource_free tunnel_initiator
```

**disable radius
resource_free tunnel_
initiator**

This command disables the resource-free tunnel initiator.

Syntax

```
disable radius resource_free tunnel_initiator
```

Example

```
disable radius resource_free tunnel_initiator
```

**enable radius
send_acct_for_default_
user**

This command enables the sending of accounting for users named “default.” This is enabled by default.

Syntax

```
enable radius send_acct_for_default_user
```

Example

```
enable radius send_acct_for_default_user
```

Related Commands

[disable radius send_acct_for_default_user](#)

[show radius settings](#)

**enable radius
source_port_
authentication**

This command indicates whether to check that the source port in the RADIUS packets received from the RADIUS authentication server are the same as configured in the router card. The default is enabled.

Syntax

```
enable radius source_port_authentication
```

Example

```
enable radius source_port_authentication
```

Related Commands

[disable radius source_port_authentication](#)

[show radius settings](#)

**enable radius
use_radius_username**

This command allows the User Name attribute in the RADIUS access_accept packet to override the default supplied in the request. The default is disabled.

Syntax

```
enable radius use_radius_username
```

Example

```
enable radius use_radius_username
```

Related Commands

[disable radius use_radius_username](#)

[show radius settings](#)

enable radius_auth_fail_traps

This command enables the authorization-failed traps.

Syntax

```
enable radius_auth_fail_traps
```

Example

```
enable radius_auth_fail_traps
```

Related Commands

[disable radius_auth_fail_traps](#)

disable radius_auth_fail_traps

This command disables the authorization-failed traps.

Syntax

```
disable radius_auth_fail_traps
```

Example

```
disable radius_auth_fail_traps
```

Related Commands

[enable radius_auth_fail_traps](#)

enable service_loss_busyout [ping | radius]

This command allows the router card to busy out modems if there is no connectivity to the ping or RADIUS server. The default is disabled.



You cannot enable both PING and RADIUS busy out features at the same time. If the PING busy-out feature is enabled and you attempt to enable RADIUS busy-out, you'll receive an error message.

Syntax

```
enable service_loss_busyout [ping | radius]
```

Example

```
enable service_loss_busyout [ping | radius]
```

Related Commands

[disable service_loss_busyout \[ping | radius\]](#)

[show service_loss_busyout settings](#)

monitor radius This command allows monitoring of realtime RADIUS activity.

Syntax

```
monitor radius
```

- Monitoring of all RADIUS packets—Displays all RADIUS packets transmitted or received by the router card.
- Monitoring of all RADIUS authentication packets—Displays all RADIUS authentication packets transmitted or received by the router card.
- Monitoring of all RADIUS accounting packets—Displays all RADIUS accounting packets transmitted or received by the router card.
- Monitoring of a specific RADIUS user—Displays any RADIUS sessions currently active for the specified user. As any new session begins for the user, monitoring will also begin.
- Monitoring of the next session that starts up—Displays results for next RADIUS session created. This option is useful if a user is having difficulty connecting and it's unclear which interface the user will connect on because of his inclusion in a hunt group. As soon as the next incoming or outgoing RADIUS connection is established, monitoring will begin. There is no differentiation on the next session—the user selects to monitor the next session and will see the next session displayed regardless of interface or user name employed.
- Monitoring of all RADIUS packets sent to or received from a specific server—Displays all traffic to and from a specified server.
- Monitor of resource management-related packets—Displays resource management-related packets.
- Exiting the monitor—Exits the program.
- Decode and Hexadecimal Display—All monitoring displays two types of data *decode* or *hexadecimal*. *Decode*, (the default), displays packets without decompression in a textual, decoded output. *Hexadecimal* displays packets with decompression in hexadecimal and any ASCII equivalent as soon as they are received or just before transmission. Both modes can be switched on the fly.

When you issue the monitor radius command, the menu displays information similar to the following:

```
HiPer>> monitor radius
```

```
HiPer RADIUS Monitor
Select a letter for one of the following options:
A) Monitor all RADIUS packets
B) Monitor all RADIUS authentication packets
C) Monitor all RADIUS accounting plackets
D) Monitor a specific user
E) Monitor next session
F) Monitor all packets to a specific server
G) Monitor resource management packets
X) Exit the monitor.
```

For each menu choice (shown in descending order), you'll see the following screens. Options can be selected by typing the letters A, B, C, etc. Both lower case and upper case letters are accepted. All selection keys are case insensitive. Follow the prompts as directed.

Option A

Option A monitors all RADIUS packets transmitted and received by the router card. When this option is selected the following menu is displayed:

```
Tracing all RADIUS packets
Decode tracing started, press H and D to toggle between
hex and decode mode
Press Escape to return to the previous screen.
```

Pressing the letters **H** or **D** toggles the *Decode* and *Hex Dump* modes. By default, RADIUS monitor starts in decode mode. At any time during tracing, pressing **H** will toggle it to Hex Dump mode; pressing **D** will toggle it back to Decode mode.

While in decode mode, pressing the **H** displays the following message:

```
Tracing changed to hex dumps; press D for decode tracing.
```

While in Hex dump mode, pressing the letter **D** displays the following message:

```
Tracing changed to decode; press H for hex tracing.
```

Pressing the **ESC** key at any time during tracing will place the monitor back in Main Menu.

Option B

Option B traces all *authentication* packets. It will not display the accounting packets. When this option is selected the following menu is displayed:

```
Tracing all RADIUS authentication packets
Decode tracing started, press H and D to toggle between
hex and decode mode
Press Escape to return to the previous screen.
```

Option C

Option C traces all *accounting* packets can be traced. It will not display authentication packets. When this option is selected the following message is displayed:

```
Tracing all RADIUS accounting packets
Decode tracing started, press H and D to toggle between hex and decode mode
Press Escape to return to the previous screen.
```

Option D

Option D traces all packets of a specific *user*. When this option is selected the following menu is displayed:

```
Monitor a specific user
Enter the user name to monitor below:
Press Esc to return to the previous screen.
Press Enter/Return to enter the name.
User Name: [           ]
```

Enter the *user name* and press ENTER. The following message is displayed.

```
Monitoring a specific user
Decode tracing started, press H and D to toggle between hex and decode mode
Press Escape to return to the previous screen.
```

Option E

Option E monitors the *next session* only. When this option is selected the following message is displayed:

```
Tracing next RADIUS session
Decode tracing started, press H and D to toggle between hex and decode mode
Press Escape to return to the previous screen.
```

Option F

Option F monitors RADIUS packets to a specific RADIUS server. When this option is selected the following menu is displayed:

```
Monitor a specific server
Enter the server name to monitor below:
Press Escape to return to the previous screen.
Press Enter/Return to enter the name.
Server Name: [          ]
```

Now type the IP Address of the RADIUS server. Note that you need to enter the IP address of the RADIUS server and host name or any other alias or the host name will not suffice.

After typing the IP address of the RADIUS server, press the ENTER key. The following message is displayed:

```
Monitoring all packets to a specific server
Decode tracing started, press H and D to toggle between hex and decode mode
Press Escape to return to the previous screen.
```

A sample Decode tracing output looks similar to the following:

```
124.32.45.65 2345 149.112.213.34 1645 1 Access-Accept
User-Name :
NAS-IP-Address :
NAS-Port :
Interface-Index :
Chassis-Call-Slot :          admin1
Chassis-Call-Span :          149.112.223.137
Chassis-Call-Channel :       0
Service-Type :                0
Login-IP-Host :               1
  Login-Service :              1
  Login-TCP-Port :              1
Session-Timeout :              6
Idle-Timeout :                 149.112.223.3
State :                          0
Class :                           23
                                   2000
                                   699
                                   GroupOne
                                   AccountOne
```

A sample Hex dump output looks similar to the following:

Source-IP	Src-Port	Destination-IP	Dest-Port Id	Packet-Type
0.0.0.0	1646	149.112.213.34	2346	

```
Outgoing PPP Data on interface: slot:3/mod:1
 2d 10 17 19 48 65 78 20 74 72 61 63 69 6e 67 20
 73 74 61 72 74 65 64 2c 20 70 72 65 73 73 20 45
53 43 41 50 45 20 74 6f 20 73 74 6f 70 3b 20 70
72 65 73 73 20 44 20 66 6f 72 20 64 65 63 6f 64
65 20 74 72 61 63 69 6e 67 2e 0d 0a
```

Source-IP	Src-Port	Destination-IP	Dest-Port Id	Packet-Type
149.112.213.34	2346	149.112.213.137	1646	

```
2f 45 00 03 01 34 5d 00 00 ff 03 6a 46 92 73 7a
```

Option G

Option G monitors all resource management packets. When this option is selected the following menu is displayed:.

```
Tracing Resource Management packets
Decode tracing started, press H and D to toggle between hex and decode mode
Press Escape to return to the previous screen.
```

**set pbus
reported_port_density**

This command configures peak modem availability across the router card slots to correlate with the RADIUS NAS-Port attribute. RADIUS uses this attribute to specify the physical slot and port a user logs in on the router card. RADIUS also uses NAS-PORT to associate filter change requests with users.

If QUADs and HDMS are mixed in the chassis, set the reported-port-density to the maximum (24).

The NAS port ID is calculated using the following formula:

slot number(0-15) x (report_port_density) + [channel(0-255)] + reported_base
(Port Density default: 256).

Syntax

```
set pbus reported_port_density <1 to 256>
```

Example

```
set pbus reported_port_density 100
```

set pbus reported_base

This command sets the base to report modem slot/span/channel settings for packet bus modems. This affects vendor-specific fields (slot and channel) in RADIUS authentication and accounting packets. For example, when this field is set to 0, the first modem on the first span in the first slot is reported as *slot=0,span=0,channel=0*. If this field were set to 1, this modem is referred to as *slot=1,span=1,channel=1*. Use [show pbus settings](#) command to display settings.

Syntax

```
set pbus reported_base [0 | 1]
```

Example

```
set pbus reported_base 1
```

set pbus trap

This command enables and disables packet bus traps.

Syntax

```
set pbus trap
  active [enable | disable]
  congestion [disable | enable]
  error [disable | enable]
  inactive [enable | disable]
  lost [disable | enable]
```

Table 175 Set Pbus Trap Command Parameters

Parameter	Description	Settings	Default
active	Enables and disables sending traps when the packet bus is activated.	enable disable	disable
congestion	Enables and disables sending traps when the packet bus is congested.	enable disable	disable
error	Enables and disables sending traps when there is an error.	enable disable	disable
inactive	Enables and disables sending packet bus traps when the packet bus is inactive.	enable disable	disable
lost	Enables and disables sending packet bus traps when the packet bus is lost.	enable disable	disable

Related Commands

[list_pbus_sessions](#)

Security Association

A Security Association (SA) is an instantiation of a security relationship between communicating peers. Both IP security protocol (IPSEC) and internet key exchange module (IKE) require and use SAs to identify the parameters of their connections.

delete sa This command deletes the specified SA. A value of 0 deletes all the SAs in the system. The [list sa](#) command displays all the valid SAs in the system. The [show sa](#) command shows the details of a security association.

Syntax

```
delete sa <0 to 2147483647>
```

Example

```
delete sa 1000
```

Related Commands

[list sa](#)

[show sa](#)

list sa This command lists all the (phase 1 and phase 2) valid SA in the system. The [show sa](#) command shows the details of a security association. Use the [delete sa](#) command to delete a specified SA.

Syntax

```
list sa
```

Example

```
list sa
```

Related Commands

[delete sa](#)

[show sa](#)

show sa This command shows the details of the SA specified. The [list sa](#) command displays all the valid SAs in the system. Use the [delete sa](#) command to delete a specified SA.

Syntax

```
show sa <0 to 2147483647>
```

Example

```
show sa 1000
```

Related Commands

[list sa](#)

[delete sa](#)

TACACS+

set tacacsplus interim_accounting_ interval

This command configures the interval in minutes to issue a watchdog accounting request to the TACACS+ server. Watchdog requests provide updated accounting information for a dialup user connection. The default is 240. The range is 5 to 3600.

Syntax

```
set tacacsplus interim_accounting_interval <5 to 3600>
```

Example

```
set tacacsplus interim_accounting_interval 100
```

Related Commands

[disable tacacsplus interim_accounting_interval](#)

show authorization settings

This command displays whether TACACS+ remote authorization is enabled or disabled. Issue the [enable authorization](#) or [disable authorization](#) commands to change the present setting.

Syntax

```
show authorization settings
```

Example

```
show authorization settings
```

Related Commands

[enable authorization](#)

[disable authorization](#)

show direct_request

This command displays all directed requests issued by TACACS+ as set by the [set direct_request timeout](#) command.

Syntax

```
show direct_request
```

Example

```
show direct_request
```

Related Commands

[set direct_request timeout](#)

show tacacsplus settings

This command displays TACACS+ watchdog accounting configuration such as the specified interval to issue an accounting watchdog request to the TACACS+ server and whether that interval service is enabled or disabled. It lists the following information:

- The Direct Req. Delimiter
- The Timeout
- Accounting Format
- Status is
- Interim Accounting Interval Status
- Interim Accounting Interval

Syntax

```
show tacacsplus settings
```

Example

```
show tacacsplus settings
```

disable authorization This command disallows TACACS+ authorization. If authorization is disabled, the router card attempts to authenticate based on the “default” user profile.

Syntax

```
disable authorization
```

Example

```
disable authorization
```

disable direct_request This command disables the TACACS+ direct request functionality configured with the [set direct_request timeout](#) command.

Syntax

```
disable direct_request
```

Example

```
disable direct_request
```

Related Commands

[enable direct_request](#)

disable tacacsplus interim_accounting_interval This command disallows watchdog accounting on the TACACS+ server.

Syntax

```
disable tacacsplus interim_accounting_interval
```

Example

```
disable tacacsplus interim_accounting_interval
```

Related Commands

[enable tacacsplus interim_accounting_interval](#)

[set tacacsplus interim_accounting_interval](#)

enable authorization This command allows TACACS+ authorization. If authorization is disabled, the router card attempts to authenticate based on the “default” user profile (username and password). The default is enabled.

Syntax

```
enable authorization
```

Example

```
enable authorization
```

Related Commands

[disable authorization](#)

[show authorization settings](#)

enable direct_request This command enables the TACACS+ directed request functionality configured with the [set direct_request timeout](#) command.

Syntax

```
enable direct_request
```

Example

```
enable direct_request
```

Related Commands

[set direct_request timeout](#)

enable tacacsplus interim_accounting_ interval

This command permits watchdog accounting on the TACACS+ server.

A TACACS+ related command useful for tunneling and global realm, allowing administrators to maintain separate AAA servers for different groups of users. The command enables the router card to direct authentication requests to a specified AAA server. The user name and password a user normally enters when connecting to the router card is expressed in the following way when employing directed request: *user@domain*. In this syntax, *user* is the *user name* and *host* the *host name* to which authentication is directed. The router card sends only the portion of the user name preceding the @ sign to the host specified following the @ sign. In other words, directed request lets you transmit a request to a configured server with only the user name sent to that specified server.

When deactivated using the [disable direct_request](#) command, AAA server rotation connects to the first available entry in the AAA Server Table via a round-robin method. The default is enabled.

Syntax

```
enable tacacsplus interim_accounting_interval
```

Example

```
enable tacacsplus interim_accounting_interval
```

Related Commands

[disable tacacsplus interim_accounting_interval](#)

[set tacacsplus interim_accounting_interval](#)

**set direct_request
timeout**

This command sets the interval from 0 to 30 seconds before the router card selects the next preferred server. The default is 5 seconds.

Syntax

```
set direct_request timeout <0 to 30>
```

Example

```
set direct_request timeout 10
```

Related Commands

[enable direct_request](#)

**add cleartcp
encryption_ids**

This command adds a ClearTCP encryption ID (up to 32 ASCII characters) and hexadecimal key.

Syntax

```
add cleartcp encryption_ids <name> key <hex number>
```

Example

```
add cleartcp encryption_ids chicago key 3A
```

Related Commands

[delete cleartcp encryption_ids](#)

**delete cleartcp
encryption_ids**

This command deletes the ClearTCP encryption IDs.

Syntax

```
delete cleartcp encryption_ids <name>
```

Example

```
delete cleartcp encryption_ids chicago
```

Related Commands

[add cleartcp encryption_ids](#)

list cleartcp encryption_ids This command lists the activation ID and the key added with the [add cleartcp encryption_ids](#) command.

Syntax

```
list cleartcp encryption_ids
```

Example

```
list cleartcp encryption_ids
```

Related Commands

[add cleartcp encryption_ids](#)

[delete cleartcp encryption_ids](#)



SIGNALING SYSTEM 7 COMMANDS

This chapter describes commands for the Total Control Hub implementation of the Signaling System 7 (SS7) External Signaling Interface Gateway (ESIG) functionality using the router card.

- [SS7 Functionality](#)
- [SS7 Commands](#)

SS7 Functionality

SS7 functionality is an optional feature that must be purchased separately. To determine if your router card has the SS7-enabled software installed enter the following CLI command:

show system settings

This command lists the following information:

- **System Descriptor**—Description of the system in use
- **Object ID**—Specific identification
- **System UpTime**—The length of time the system has been up
- **System Contact**—Name of the system contact
- **System Name**—The name given to the system
- **System Location**—The location of the system
- **System Services**—Description of what the system does
- **System Transmit Authentication Name**—The authentication name given to the system
- **System Version**—The version of the system in use. If the **System Version** ends with **SS7**, your router card is SS7-enabled.
- **Reset EEPROM Settings On Bootup**—Whether or not the EEPROM settings will be reset upon bootup of the system.

Syntax

```
show system setting
```

SS7 Commands

The protocol monitor utility can be used to monitor the SS7 signaling. Use the command **monitor protocol** to enter the protocol monitor utility. From the list displayed, enter the letter that corresponds to SS7.

connect ss7 gateway

If the startup method is set to manual and the connection status is down, use this command to manually connect to the SS7 gateway. The router card always tries to make the SLAP connection to the Primary gateway first. The number of times the router card tries to make the connection is set by the command **set ss7 slap_v2 gateway_retry_count**. The secondary gateway is then tried for the same number of times, and if no connection is made, the primary gateway is tried again. This method continues until a connection is established.

Syntax

```
connect ss7 gateway
```

Related Commands

[show ss7 slap status](#)

[set ss7 protocol \[slap_v2\]](#)

**connect ss7 slot
<slot_list>**

Use this command to manually connect to a specified SS7 slot if the connection to the gateway is up and the router card is the owner of the signaling slot. Use the [list ss7 slots](#) command to verify ownership of the slot.

Syntax

```
connect ss7 slot <slot_list>
```

Related Commands

[list ss7 slots](#)

**disable ss7
slap_down_trap**

This command disables sending an SNMP trap when SLAP signaling goes down.

Syntax

```
disable ss7 slap_down_trap
```

**disable ss7
slap_up_trap**

This command disables sending an SNMP trap when SLAP signaling goes up.

Syntax

```
disable ss7 slap_up_trap
```

disable ss7 slot_down_trap This command disables sending SNMP trap when connection to HDM goes down.

Syntax

```
disable ss7 slot_down_trap
```

disable ss7 slot_up_trap This command disables sending SNMP trap when connection to HDM goes up.

Syntax

```
disable ss7 slot_up_trap
```

disable ss7 trace This command disables SLAP or slot side tracing.

Syntax

```
disable ss7 trace [slap | slots <slot_list>]
```

Table 176 Disable SS7 Trace Command Parameters

Parameter	Description
slap	Disable the SLAP side tracing.
slots	Disable side tracing for a particular slot. To designate all slots enter the range 1-16 as the slot number. Enter a list or range of slots for this value.

disconnect ss7 gateway This command disconnects from the SS7 gateway.

Syntax

```
disconnect ss7 gateway
```

disconnect ss7 slot This command disconnects the specified SS7 slots. The value <slot_list> is a value from 1 to 16. A range of 1 to 16 disconnects all slots.

Syntax

```
disconnect ss7 slot <slot_list>
```

enable ss7 slap_down_trap This command enables sending an SNMP trap when SLAP signaling goes down.

Syntax

```
enable ss7 slap_down_trap
```

enable ss7 slap_up_trap This command enables sending an SNMP trap when SLAP signaling goes up.

Syntax

```
enable ss7 slap_up_trap
```

enable ss7 slot_down_trap This command enables sending SNMP trap when connection to HDM goes down.

Syntax

```
enable ss7 slot_down_trap
```

enable ss7 slot_up_trap This command enables sending SNMP trap when connection to HDM goes up.

Syntax

```
enable ss7 slot_up_trap
```

enable ss7 trace This command enables SLAP or slot side tracing.

Syntax

```
enable ss7 trace [slap | slots <slot_list>]
```

Table 177 Enable SS7 Trace Command Parameters

Parameter	Description
slap	Enable the SLAP side tracing.
slots	Enable SBUS side tracing for a particular slot. Enter a list or range of slots for this value. For all slots use 1-16 .

list ss7 slots This command lists the following SS7 slot configuration:

- Slot
- Owner
- Type
- Connection Status
- Down Reason

Syntax

```
list ss7 slots
```

reset ss7 counters This command resets the SS7 counters.

Syntax

```
reset ss7 counters
```

send ss7 heartbeat This command sends an SS7 heartbeat to an SS7 gateway.

Syntax

```
send ss7 heartbeat
```

Related Commands

[set ss7 protocol \[slap_v2\]](#)

[set ss7 slot](#)

[set ss7 protocol \[slap_v2\]](#)

**set ss7 protocol
[slap_v2]**

This command sets the protocol used to communicate with SS7 gateways.



At this time only the SLAP V2 protocol is supported for communication with SS7 gateways.

Syntax

```
set ss7 protocol [slap_v2]
    chassis_id <Hexadecimal number>
    drop_call_on_signal_loss [disabled | enabled]
    drop_call_timer <1 to 4294967295>
    gateway_retry_count <1 to 65535>
    gateway_retry_interval <1 to 65535>
    heartbeat_threshold <0 to 65565>
    heartbeat_timer_far_end <1 to 4294967295>
    heartbeat_timer_near_end <1 to 4294967295>
    primary_host <ip_name_or_addr>
    primary_host_port <port>
    secondary_host <IP name or address>
    secondary_host_port <port>
```

Table 178 Set SS7 Protocol Slap_v2 Command Parameters

Parameter	Description
chassis_id	The chassis ID of the router card in the form of any Hexadecimal number.
drop_call_on_signal_loss	When enabled, calls are dropped if the signaling connection is lost and not regained within the time specified by drop_call_timer.
drop_call_timer	The amount of time in milliseconds to wait before dropping calls when the signaling connection is lost. Range: 0 to 4294967294 ms. Default: 0 ms.
gateway_retry_count	The number of times to retry connecting to a gateway. The range is from 0 to 65535. Default is 3.
gateway_retry_interval	How long, in seconds, to wait between retries. The range is from 1 to 65535 seconds. Default is 2 seconds.
heartbeat_threshold	The maximum number of time-out that may pass without receiving a heartbeat. One timeout is the missing of a heartbeat during the entire time of heartbeat_timer_far_end. A value of 0 (zero) means no timeout allowed and there will be no attempt at connection re-establishment. The Gateway is disconnected immediately and if the startup method is set to auto, the retry algorithm is executed. The range is from 0 to 65535. Default is 1.
heartbeat_timer_far_end	The time, in milliseconds, when the far end sends a heartbeat. If the heartbeat is not received in this specified time it is taken as a timeout. The range is from 1 to 4294967295. Default is 16000 ms.
heartbeat_timer_near_end	The frequency for the local heartbeat timer in milliseconds. The range is from 1 to 4294967295. Default is 14000ms.

Table 178 Set SS7 Protocol Slap_v2 Command Parameters

Parameter	Description
primary_host	The IP address or network name of the primary SS7 gateway.
primary_host_port	The IP port to use on the primary SS7 gateway.
secondary_host	The IP address or network name of the secondary SS7 gateway.
secondary_host_port	The IP port to use on the secondary SS7 gateway.

set ss7 slot This command sets the SS7 slot, owner, and type.

Syntax

```
set ss7 slot <list>
      owner [no | yes]
      type [dynamic | static]
```

set ss7 This command sets SS7 parameters by slot number, configuring the ownership of the HDMs in the chassis for SS7 signal handling.

Syntax

```
set ss7
      startup_method [auto | manual]
      trace_output [screen | syslog]
```

Table 179 Set SS7 Command Parameters Descriptions

Parameter	Description
list	The slot list can be a list of individual slots (1, 3, 5) or a range of slots (1-5).
owner	If set to yes, slap signaling for that slot will be done by the router card.
type	If static, discards the chassis awareness for this slot. If dynamic, maintains the chassis awareness for this slot.
startup_method	auto—sets the start method to auto. The router card starts a connection to the ss7 gateway immediately after booting up. similarly if the connection goes away HARC will try to reconnect automatically. manual—user has to manually initiate the connection to the gateway using the command 'connect gateway'
trace_output	screen—displays the trace output to the screen. Also see enable ss7 trace. syslog—sends the trace output only to syslog. Also see enable ss7 trace.

show ss7 This command displays the current configuration of the SS7, consisting of the following information:

- SS7 Protocol
- SS7 Startup Method
- SLAP Primary and Secondary Gateways and Ports
- SLAP Heartbeat Timer Far End, Near End, and Threshold
- SLAP Chassis ID
- SLAP Gateway Connection Retries and Interval
- Drop Call On Signal Loss
- Drop Call Timer

Syntax

```
show ss7 settings
```

show ss7 counters This command shows the counter values for the SS7, consisting of the following:

- Counters Start Time
- Packets Transmitted to and Received from SBUS
- Bytes and Packets Transmitted to GW
- Bytes and Packets Received from GW
- Heartbeats Missed

Syntax

```
show ss7 counters
```

show ss7 slap status This command shows the status of the signaling connection, consisting of the primary and secondary gateway status and the gateway down causes.

Syntax

```
show ss7 slap status
```

**show ss7 slot
<slot_list> counters**

This command displays the following counters for a specified slot:

- SBUS transmit OK count
- SBUS transmit Fail count
- SBUS receive OK count
- SBUS receive Fail count

Syntax

```
show ss7 slot <slot list> counters
```

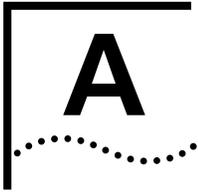
show ss7 trap status

This command shows the status of the present trap configuration. When enabled, SNMP traps are sent in the following cases:

- When the SLAP connection (gateway) goes up or down
- When the slot connection goes up or down

Syntax

```
show ss7 trap status
```

ALPHABETICAL COMMAND LISTING

add aaa_server 467
add address_pool user 166
add atm_arp_server 299
add atm1483 pvc 307
add atm1577 pvc 308
add chat_script 58
add cleartcp encryption_ids 529
add cross_connect 239
add cross_connect 363
add datalink frame_relay interface <interface_name> 378
add datalink ppp user <username> 425
add dns host 365
add dns server 365
add filter 483
add frame_relay ptmp_pvc_group 376
add frame_relay pvc 375
add framed_route user 317
add framed_route user 379
add init_script 273
add ip arp address <IP address> access_mac_address <MAC address> interface <interface name> 300
add ip arp address <IP address> state [private | public] 301
add ip defaultroute gateway 313
add ip invarp <IP address> type [dynamic | static] 305
add ip network 314
add ip pool 209
add ip route 316
add ip source route <IP or net addr> gateway <IP name or addr> metric <metric> 317
add ipx network 318
add ipx route 319
add ipx service 320
add l2tp lns <1 to 9> address <IP address> 445
add logical_ds1 interface 243
add login_host 175
add login_table 177
add modem_group 227
add mpip client 211
add mpip server 212
add network service 231
add ospf cryptographic_key <key_id> 398
add ospf receivepolicy 399
add ospf sendpolicy 401
add ping service_loss_system 183
add policy 478
add pppoe service_name 437
add pptp pns <1-9> address <IP address> 460
add rshd clients 191
add snmp community 192
add snmp community_pool 193
add snmp trap_community 194
add snmp trap_community_pool 195
add syslog 71
add tap interface 291
add tap next 293
add tap user 294
add telnet client 144
add tftp client 203
add tftp request 204
add user 147
arp 301
assign interfaces 243
assign interfaces 228
cfp_delay_command 67
clear arp_cache 301
close 142
Command Completion 52
Command Line Edit 51
Command Retrieval 52
connect 141
connect ss7 gateway 532
connect ss7 slot <slot_list> 532
copy file 114
Default User 45
delete aaa_server <name> preference <number> 469
delete aaa_server 469
delete address_pool user 167
delete atm_arp_server 302
delete atm1483 pvc 309
delete atm1577 pvc 309
delete board crashdump 70
delete chat_script 60
delete cleartcp encryption_ids 529
delete configuration 113
delete cross_connect 240
delete datalink frame_relay interface 379
delete datalink ppp interface 425
delete dns cache 366
delete dns host 366
delete dns ncache 367
delete dns server preference 367
delete file 114
delete filter 484
delete frame_relay pvc 379
delete framed_route user 379
delete init_script 274
delete ip arp address <IP address> interface <interface name> 302
delete ip defaultroute gateway 322
delete ip invarp 305
delete ip network 322
delete ip pool 323
delete ip route 323
delete ip source route 324
delete ip source route 80

delete ipx network 324
delete ipx route 324
delete ipx service 325
delete ipx service_all 325
delete l2tp lns 445
delete logical_ds1 interface 244
delete login_host preference 176
delete login_table 178
delete modem_group 229
delete mpip client 393
delete mpip server 393
delete network service 236
delete ospf cryptographic_key 403
delete ospf default_area 403
delete ospf receivepolicy <network_address/ mask> 403
delete ospf sendpolicy 404
delete ping row 184
delete ping service_loss_system 185
delete policy 478
delete pppoe service_name 438
delete pptp pns 462
delete rshd clients 191
delete sa 524
delete snmp community 195
delete snmp community_pool 196
delete snmp trap_community 196
delete snmp trap_community_pool 196
delete syslog 72
delete tap 295
delete tap id 296
delete telnet client 144
delete tftp client 205
delete tftp request 205
delete traceroute row 138
delete user 148
dial 225
dialout l2tp 225
dialout pptp 226
disable accounting 507
disable accounting server_group 508
disable atm_arp_server 303
disable atm1483 pvc 309
disable atm1577 pvc 310
disable atmsig 310
disable authentication 472
disable authorization 527
disable auto_answer 270
disable call_reject_code 269
disable chassis contiguous_modem_naming 273
disable command global_terminal_settings_page_breaks 62
disable command local_terminal_settings_page_breaks 63
disable critical_events_to_flash 78
disable cross_connect 364
disable datalink frame_relay interface 380
disable datalink ppp interface 428
disable direct_request 527
disable dns host_rotation 367
disable dns round_robin 367
disable frame_relay pvc 380
disable health_trap 118
disable icmp logging 392
disable icmp logging 73
disable icmp router_advertise 391
disable ilmi 426
disable interface 244
disable ip 325
disable ip address_pool_round_robin 327
disable ip address_pool_filtering 326
disable ip forwarding 327
disable ip_ia_force_nexthop_route 327
disable ip_ia_next_hop_routing 328
disable ip_multicast_heartbeat 328
disable ip_network 329
disable ip_proxy_arp_all_dialin 329
disable ip_rip 329
disable ip_routing 330
disable ip_security_option 481
disable ip_send_host_unreach_for_pool 330
disable ip_send_unsolicited_arp 330
disable ip_source_address_filter 331
disable ip_static_remote_routes 331
disable ipx_network 331
disable ipx_rip_network 332
disable ipx_sap_network 332
disable L2TP_force_multiple_tunnels 458
disable l2tp_lcp_renegotiation_at_lns 446
disable l2tp_lns 446
disable L2TP_use_client_auth_id_for_assignment_id 458
disable link_traps interface 197
disable modem_group 229
disable network service 236
disable nmc_chassis_awareness 282
disable nmc_dsa_idle_rebalancing 282
disable nmc_dynamic_slot_assignment 283
disable nmc_snmp_forwarding 283
disable ntp 223
disable ospf 405
disable ospf_area 405
disable ospf_interface 405
disable ping_service_loss_system 185
disable ppp_acct_for_abnormal_disc 426
disable ppp_address_field_compression 426
disable ppp_bacp_bap 427
disable ppp_multilink_ppp 427
disable ppp_negotiated_callback 477
disable ppp_offloading 427
disable ppp_protocol_field_compression 428
disable ppp_radius_challenge_with_pap 432
disable ppp_receive_accm 428
disable ppp_send_edo 437
disable pppoe_on_interface 438
disable pptp_pns 462
disable primary_accounting_server 502
disable prioritize_first_accounting_server_in_a_group 504
disable prompting_single_level 178
disable radius_accounting 508
disable radius_auth_fail_traps 517
disable radius_fill_null_attributes 509
disable radius_ignore_source_port 513
disable radius_interim_accounting_interval 509
disable radius_resource_free_tunnel_initiator 515
disable radius_resource_management 509
disable radius_send_acct_for_default_user 510
disable radius_send_unauth_acct_record 514
disable radius_source_port_authentication 510
disable radius_use_radius_username 510

disable rlogin escape 178
disable secondary_accounting_server 504
disable security_option remote_user_administration 167
disable security_option snmp_user_access 197
disable service_loss_busyout [ping | radius] 511
disable slip offloading 237
disable snmp authentication traps 197
disable ss7_slap_down_trap 532
disable ss7_slap_up_trap 532
disable ss7_slot_down_trap 533
disable ss7_slot_up_trap 533
disable ss7_trace 533
disable syslog_event_log 73
disable system_reset_eeprom 70
disable tacacsplus_interim_accounting_interval 527
disable tcp_keepalives 168
disable tcp_nagle_algorithm 168
disable telnet 145
disable telnet_disconnect_message 144
disable tftp_request 205
disable tunnel_switch 464
disable user 148
disable vtp_timestamp_checking 466
disconnect l2tp_tunnel <number> session <number> 446
disconnect l2tp_tunnel 446
disconnect pptp <number> session <number> 463
disconnect pptp_tunnel <number> 462
disconnect ss7_gateway 533
disconnect ss7_slot 533
disconnect user 149
disconnect vtp_tunnel 466
do 66
edit 114
enable accounting 511
enable accounting_server_group [a | b] 511
enable atm_arp_server 303
enable atm1483_pvc 428
enable atm1577_pvc 429
enable atmsig 429
enable authentication 472
enable authorization 528
enable auto_answer 270
enable call_reject_code 269
enable chassis_contiguous_modem_naming 272
enable command_global_terminal_settings_page_breaks 61
enable command_local_terminal_settings_page_breaks 62
enable critical_events_to_flash 78
enable cross_connect 240
enable cross_connect 364
enable datalink_frame_relay_interface 380
enable datalink_ppp_interface 430
enable direct_request 528
enable dns_host_rotation 368
enable dns_round_robin 368
enable frame_relay_pvc 381
enable health_trap 118
enable icmp_logging 74
enable icmp_router_advertise 391
enable ilmi 430
enable interface 244
enable ip 333
enable ip_address_pool_round_robin 334
enable ip_address_pool_filtering 334
enable ip_forwarding 334
enable ip_ia_force_next_hop_route 335
enable ip_ia_next_hop_routing 335
enable ip_multicast_heartbeat 335
enable ip_network 336
enable ip_proxy_arp_all_dialin 336
enable ip_rip 337
enable ip_routing 337
enable ip_security_option 479
enable ip_send_unsolicited_arp 337
enable ip_source_address_filter 338
enable ip_static_remote_routes 338
enable ipx_network 339
enable ipx_rip_network 339
enable ipx_sap_network 339
enable L2TP_force_multiple_tunnels 458
enable l2tp_lcp_renegotiation_at_lns 447
enable l2tp_lns 447
enable L2TP_use_client_auth_id_for_assignment_id 458
enable link_traps_interface 198
enable modem_group 275
enable network_service 237
enable nmc_chassis_awareness 283
enable nmc_dsa_idle_rebalancing 284
enable nmc_dynamic_slot_assignment 284
enable nmc_snmp_forwarding 284
enable ntp 223
enable ospf 406
enable ospf_area 406
enable ospf_interface 406
enable ping_service_loss_system 185
enable ppp_acct_for_abnormal_disc 430
enable ppp_address_field_compression 430
enable ppp_bacp_bap 431
enable ppp_multilink_ppp 431
enable ppp_negotiated_callback 477
enable ppp_offloading 431
enable ppp_protocol_field_compression 432
enable ppp_radius_challenge_with_pap 432
enable ppp_receive_accm 431
enable ppp_send_edo 437
enable pppoe_on_interface 438
enable pptp_pns 462
enable primary_accounting_server 503
enable prioritize_first_accounting_server_in_a_group 503
enable prompting_single_level 179
enable radius_accounting 512
enable radius_auth_fail_traps 517
enable radius_authentication_syslog_counters 512
enable radius_fill_null_attributes 514
enable radius_ignore_source_port 513
enable radius_interim_accounting_interval 514
enable radius_resource_free_tunnel_initiator 515
enable radius_resource_management 515
enable radius_send_acct_for_default_user 516
enable radius_send_unauth_acct_record 513
enable radius_source_port_authentication 516
enable radius_use_radius_username 516
enable rlogin_escape 179
enable secondary_accounting_server 503
enable security_option_remote_user_administration 167
enable security_option_snmp_user_access 198
enable service_loss_busyout [ping | radius] 517

enable slip offloading 238
enable snmp authentication traps 198
enable ss7 slap_down_trap 534
enable ss7 slap_up_trap 534
enable ss7 slot_down_trap 534
enable ss7 slot_up_trap 534
enable ss7 trace 534
enable syslog event_log 73
enable system reset_eeprom 71
enable tacacsplus interim_accounting_interval 528
enable tcp keepalives 168
enable tcp nagle_algorithm 169
enable telnet 145
enable telnet disconnect_message 144
enable tftp request 206
enable tunnel switch 464
enable user 149
enable vtp timestamp checking 466
Ending a Process 52
exit 141
hangup interface 245
hangup modem_group 276
help 141
help 143
Help 42
help 53
hide events 79
history 53
host <IP_host_name> 369
Interface Names 44
Interface Ranges 44
invarp ptmp_pvc_group 306
invarp pvc 306
join ip igmp <IP_multicast_address> 395
kill 54
leave 69
leave ip igmp <IP_multicast_address> 395
list aaa_server 469
list active interfaces 245
list all sessions vpn 440
list all tunnels 440
list atm1483 pvcs 310
list atm1577 pvcs 311
list available servers 237
list chassis 113
list chat_scripts 60
list cleartcp encryption_ids 530
list connections 246
list critical events 79
list cross_connect 241
list cross_connect 364
list dhcp_proxy leases 174
list dnis_connections 370
list dns cache 369
list dns hosts 370
list dns ncache 371
list dns servers 371
list ds_one interfaces 245
list facilities 116
list files 115
list filters 484
list frame_relay 381
list frame_relay ptmp_pvc_group 376
list init_scripts 274
list interfaces 247
list ip addresses 80
list ip aggregate_routes 212
list ip arp 304
list ip defaultroute 81
list ip igmp 395
list ip interface_block 247
list ip invarp network 306
list ip networks 340
list ip pools 340
list ip routes 341
list ip source routes 342
list ip static_arp 342
list ipx networks 343
list ipx routes 343
list ipx services 344
list ipx static routes 345
list l2tp lns 447
list l2tp session_counters 449
list l2tp sessions tunnel 449
list l2tp tunnels 448
list lan interfaces 345
list login_hosts 179
list login_sessions 180
list login_table 177
list modem_groups 230
list mpip bundles 213
list mpip clients 213
list mpip links 213
list mpip locallinks 214
list mpip servers 214
list nat sessions 482
list nat stats 482
list network 115
list network services 234
list ospf 407
list ospf cryptographic_key 407
list ospf host 408
list ospf interface 408
list ospf lsdb all 409
list ospf neighbor 409
list ospf receivepolicy 410
list ospf sendpolicy 410
list pbus datagrams 135
list pbus sessions 286
list pbus traps 287
list ping service_loss_systems 185
list ping systems 186
list policy 116
list ppp 345
list pppoe 439
list pptp pnss 463
list pptp tunnel <number> sessions 463
list pptp tunnels 464
list processes 116
list rshd clients 192
list rtab preferred 117
list sa 524
list sessions 97
list sessions counters 97
list snmp communities 199
list snmp community_pools 199

list snmp trap_communities 200
list snmp trap_community_pools 200
list ss7 slots 535
list switched interfaces 248
list sync interfaces 248
list syslogs 74
list tap 295
list tcp connections 169
list telnet clients 146
list tftp clients 206
list tftp requests 134
list timezone 57
list traceroute 137
list traceroute row <number> hops 138
list tunnel connections 440
list udp listeners 99
list users 150
list virtual connections 439
list vpn <0 to 65535> vtp tunnels 466
list vtp tunnels 466
logout 141
logout 69
manage 141
monitor ppp 432
monitor protocol 82
monitor radius 518
Names 44
Network Address Formats 43
Output Pause 52
Parameters 40
ping 187
Positional Help 52
quit 69
reboot 54
reconfigure ip network 81
rename file 115
reset 95
reset l2tp session_counters 449
reset ss7 counters 535
reset statistics 96
reset syslog event_log 73
resolve name 180
rlogin 142
rlogin 181
save all 54
save configuration 55
send 143
send ss7 heartbeat 535
set aaa_server 470
set accounting 489
set accounting call_detail_record [disabled | enabled] 496
set accounting server_group [a | b] retransmissions 498
set accounting_backup primary 492
set accounting_backup secondary 494
set acct_format [all | simple | sprint] 498
set atm options 311
set atm_address network 312
set authentication 473
set board command_line_parameters 67
set bootrom boot interface 67
set bootrom config 67
set bootrom ip interface 68
set bulk_file 58
set chassis slot <slot_list> console [no | yes] 272
set chassis slot 271
set clearTCP connect_message 170
set command 63
set connection 214
set datalink frame_relay interface 288
set date 55
set dhcp_proxy 173
set dialout user <user name> site 154
set dialout user 153
set dialout user 226
set direct_request timeout 529
set dns 372
set dns server preference 373
set ds1 interface 249
set escape 143
set facility 75
set frame_relay conformance 382
set frame_relay interface 383
set frame_relay pvc <pvc_name> 385
set frame_relay trap_min_interval 382
set frame_relay traps 382
set framed_route user 156
set global_call_type 441
set health_trap interval 118
set init_script 275
set interface 485
set ip application_source_address 346
set ip arp address 347
set ip defaultroute gateway 347
set ip defaultroute metric 347
set ip igmp [eth:1 | eth:2 | slot:x/mod:y] 396
set ip multicast heartbeat 394
set ip multicast proxy interface 394
set ip network <name> 348
set ip pool 216
set ip route <IP_hostname or network address> 351
set ip routing 352
set ip source route 353
set ip source_based_routing 353
set ip unnumbered_link local_address <IP address> 354
set ipx network 355
set ipx system 217
set l2tp 450
set l2tp lns 451
set logical_ds1 interface 251
set login user 156
set login_host preference 181
set login_table <name> 182
set maximum_local_users 158
set modem_group 276
set mpip 221
set mpip client 221
set mpip server 222
set network service 235
set network user <name> ip 160
set network user <user name> igmp 159
set network user <user name> ipx 162
set network user <user name> ppp 163
set network user <user_name> ppp_source_ip_filter [enabled | disabled] 165
set network user 158
set ntp 224

set ospf area 411
set ospf cryptographic_key 412
set ospf default_area_id 413
set ospf global 413
set ospf host 414
set ospf interface 415
set ospf receivepolicy <network_address/ mask> 416
set ospf sendpolicy 418
set packet_logging 486
set pbus reported_base 523
set pbus reported_port_density 523
set pbus trap 523
set ping maximum_rows 188
set ping service_loss_system 189
set policy update 488
set ppp 219
set pppoe 439
set pptp <number> 459
set radius 499
set security_service 502
set service_loss_busyout radius frequency 502
set slip session_start_message 238
set snmp community 201
set snmp trap_community 202
set ss7 537
set ss7 protocol [slap_v2] 536
set ss7 slot 537
set switched interface 252
set sync interface 258
set syslog 76
set syslog_format 77
set system 64
set tacacsplus interim_accounting_interval 525
set tap id 296
set tap user 297
set tcp keepalive_interval 171
set tcp maximum_connections 171
set telnet admin_banner_file 142
set tftp request 206
set time 56
set timezone 56
set traceroute maximum_rows 138
set tunnel user 165
set user 150
show aaa_server <name> preference <number> 471
show accounting 504
show accounting counters 101
show accounting server_group [a | b] counters 101
show all active interfaces 83
show all configuration output 66
show all configuration settings 83
show all connections 83
show all filters 84
show all interfaces 84
show all ip networks 84
show all ipx networks 84
show all l2tp tunnels 84
show all lan interfaces 84
show all networks 84
show all ospf areas 85
show all ospf interfaces 85
show all sessions 85
show all switched interfaces 85
show all users 85
show all vpn 86
show all vtp tunnels 86
show atm counters [ds3:x | e3:x | atmcell:x] 102
show atm_arp_server 304
show atm1483 pvc <name> settings 312
show atm1577 pvc <name> settings 313
show atmcfg 313
show authentication counters 103
show authentication server_status 104
show authentication settings 102
show authentication settings 475
show authorization settings 526
show auto_answer 271
show board command_line_parameters 87
show board crashdump 70
show board settings 87
show bootrom ip interface 260
show bootrom settings 87
show bulk_file 115
show bulk_file 58
show call reject_code status 270
show chassis slot <slot number> 113
show chat_script 61
show clearTCP 171
show command settings 88
show configuration settings 88
show connection counters 105
show connection settings 104
show contact 506
show contact timers 506
show cpu utilization 89
show critical_event settings 114
show cross_connect 240
show cross_connect 364
show datalink frame_relay interface <interface name> lmi statistics 112
show datalink frame_relay interface <interface_name> counters 111
show datalink frame_relay interface <interface_name> counters 288
show datalink frame_relay interface <interface_name> lmi statistics 289
show datalink frame_relay interface <interface_name> settings 390
show date 57
show date 89
show dhcp_proxy counters 175
show dhcp_proxy settings 174
show direct_request 526
show dns cache 374
show dns counters 105
show dns ncache 375
show dns settings 373
show ds1 interface <physical_interface_name> ch_map 261
show ds1 interface <physical_interface_name> current_tbl 262
show ds1 interface <physical_interface_name> fend_current_tbl 263
show ds1 interface <physical_interface_name> fend_interval_tbl 264
show ds1 interface <physical_interface_name> fend_total_tbl 264
show ds1 interface <physical_interface_name> interval_tbl 265
show ds1 interface <physical_interface_name> total_tbl 266
show ds1 interface 251

show events 75
show events 79
show file 89
show filter 487
show frame_relay interface <interface_name> counters 107
show frame_relay interface <interface_name> lmi statistics 108
show frame_relay interface <interface_name> settings 386
show frame_relay ptmp_pvc_group <net name> counters 376
show frame_relay ptmp_pvc_group <net name> settings 377
show frame_relay pvc <net name> counters 378
show frame_relay pvc <net name> settings 377
show frame_relay pvc <pvc_name> counters 109
show frame_relay pvc <pvc_name> settings 388
show frame_relay stack 389
show global_call_type settings 441
show gre counters 117
show health_trap 118
show icmp 392
show icmp counters 118
show icmp settings 392
show interface <interface name> settings 266
show interface <interface_name> counters 120
show ip counters 121
show ip igmp [eth:1 | eth:2 | slot:x/mod:y] 397
show ip invarp 305
show ip network <network_name> settings 359
show ip network settings 358
show ip rip counters 122
show ip routing settings 360
show ip security settings 480
show ip settings 357
show ip source_based_routing <interface_name> 360
show ipx 360
show ipx counters 122
show ipx network <network name> settings 361
show ipx network <network_name> counters 123
show ipx rip counters 124
show ipx rip settings 363
show ipx sap counters 124
show ipx sap settings 363
show l2tp counters 124
show l2tp counters 454
show l2tp lns 454
show l2tp settings 452
show l2tp tunnel <number> session <number> 456
show l2tp tunnel 454
show logical_ds1 interface <logical_interface_name> ch_map 268
show maximum_local_users 89
show memory 90
show memory utilization 90
show modem_group 230
show mpip settings 223
show network <name> counters 116
show network <name> settings 116
show network 91
show nmc counters 126
show nmc settings 286
show nmc status 113
show ntp settings 225
show ospf 419
show ospf area <area_id> counters 126
show ospf area <area_id> settings 419
show ospf cryptographic_key 420
show ospf global counters 127
show ospf global settings 421
show ospf interface <IP address or IF index> counters 423
show ospf interface <IP address or IF index> settings 422
show ospf lsdB 424
show ospf receivepolicy <network_address> 424
show ospf sendpolicy <IP address> source 402
show ospf sendpolicy 425
show packet_logging 91
show pbus settings 287
show ping row <row_number> counters 128
show ping row 190
show ping server <host name or IP address> counters 129
show ping server <host name or IP address> settings 191
show ping server settings 190
show ping settings 189
show ppp on interface <slot:x/mod:y> counters 98
show ppp settings 436
show pppoe [counters | settings] 129
show pppoe 438
show pptp counters 129
show pptp settings 461
show pptp tunnel <number> session <number> 443
show pptp tunnel 441
show prompting 183
show radius 506
show radius resource_management counters 507
show radius resource_management settings 506
show remote user 91
show rs232 interface 290
show rshd counters 132
show sa 525
show security_option 480
show service_loss_busyout settings 507
show session 92
show slip settings 239
show snmp community_pool 203
show snmp counters 132
show snmp settings 202
show snmp trap_community_pool 203
show ss7 538
show ss7 counters 538
show ss7 slap status 538
show ss7 slot <slot_list> counters 539
show ss7 trap status 539
show statistics 93
show sync interface 287
show syslog 77
show syslog_format 77
show system 93
show system settings 531
show tacacsplus settings 526
show tcp 172
show tcp counters 97
show telnet settings 146
show tftp request 134
show time 57
show traceroute row <number> settings 139
show traceroute settings 139
show tunnel_switch_counters 465
show tunnel_switch settings 465
show udp counters 99
show user 157

show vtp 100
status 143
Syntax, Examples, and Related Commands 41
telnet <IP_name or address> TCP_port <number> 140
telnet 142
tftp 207
Total Control 1000 Enhanced Data System xxxiv
Total Control HiPer System xxxiv
traceroute 135
unassign interface <interface_name_list> modem_group
<group_name> 269
Users 45
Using Control Characters 41
verify chat_script 59
verify filter 488

INDEX

A

Accounting Server
 disable primary_accounting_server 503
 disable
 prioritize_first_accounting_server_in_a_group 504
 disable secondary_accounting_server 504
 enable
 prioritize_first_accounting_server_in_a_group 503
 enable secondary_accounting_server 503

Add Commands
 add aaa_server 467
 add address_pool user 166
 add atm_arp_server 299
 add atm1483 pvc 307
 add atm1577 pvc 308
 add chat_script 58
 add cross_connect 239
 add datalink frame_relay interface 378
 add dns host 365
 add dns server 365
 add filter 483
 add frame_relay pvc 375
 add framed_route user 317
 add init_script 273
 add ip defaultroute gateway 313
 add ip network 314
 add ip pool 209
 add ip route 316
 add ip source route 317
 add ipx network 318
 add ipx route 319
 add ipx service 320
 add l2tp lns address 365, 445
 add logical_ds1 interface 243
 add login_host 175
 add login_table 177
 add modem_group 227, 228
 add mpip client 211
 add mpip server 212
 add network service 231
 add ospf cryptographic_key 398
 add ospf receivepolicy 399
 add ospf sendpolicy 401
 add ping service_loss_system 183
 add policy 478
 add pppoe service_name 437
 add rshd clients 191
 add snmp community 192
 add snmp community_pool 193
 add snmp trap_community 194
 add snmp trap_community_pool 195
 add syslog 71
 add tap interface 291
 add tap next 293
 add tap user 294

 add telnet client 144
 add tftp client 203
 add tftp request 204
 add user 147

ARP Commands
 list ip arp 304

Arp Commands
 clear arp_cache 301
 delete atm_arp_server 302
 delete ip arp address interface 302
 disable atm_arp_server 303
 disable ip send_unsolicited_arp 330
 enable atm_arp_server 303
 list ip arp 304
 list ip static_arp 342
 show atm_arp_server 304

Assign Command
 assign interfaces 228, 243

Assigning users to configured address pools 166

ATM Commands
 add atm_arp_server 299
 add atm1483 pvc 307
 add atm1577 pvc 308
 delete atm1483 pvc 309
 delete atm1577 pvc 309
 disable atm1483 pvc 309
 disable atm1577 pvc 310
 disable atmsig 310
 enable atm1483 pvc 428
 enable atm1577 pvc 429
 enable atmsig 429
 list atm1483 pvcs 310
 list atm1577 pvcs 311
 set atm options 311
 set atm_address network 312
 show atmcfp 313

auto_answer 270

B

Backup IP default route, reconfiguring 347

Boot Configuration Menu
 retrieving configuration from Flash 50

C

case sensitivity in commands 43

cfp_delay_command 67

Chassis Commands
 disable nmc chassis_awareness 282
 enable nmc chassis_awareness 283
 list pbus datagrams 135
 list pbus sessions 286
 set chassis slot 271
 set chassis slot console 272

Chat Script Commands
 add chat_script 58
 delete chat_script 60
 list chat_scripts 60

 show chat_script 61

CLI mask signifier 43

close 142

Command Features 51
 Command Completion 52
 Command Line Edit 51
 Command Retrieval 52
 Ending a Process 52
 Output Pause 52
 Positional Help 52

Command Line Interface (CLI)
 abbreviating 46
 case-sensitive commands 46
 comma separation 47
 command completion 47
 command language structure 45
 command reprint 48
 command retrieval 48
 concepts 39
 deleting 49
 disabling 49
 editing 48
 features
 abbreviation 42
 additional conventions 43
 command completion 42
 command line edit 41
 command retrieval 42
 control characters 41
 help 42
 parameters 40
 position-independent arguments 41
 range of values 40
 values 40
 help 49
 keywords 46
 paused output 48
 quotations 47
 rebooting 50
 save all command 49
 saving changes 49
 syntax 47
 using
 add & set commands 50
 do & kill commands 49
 list & show commands 50
 network services 49
 vertical line 47

Commands
 cfp_delay_command 67

commands
 abbreviating 42
 aborting 41
 add 50
 case sensitivity 43
 defining strings 43
 do 49
 kill 49
 list 50

- reboot 50
- reconfigure ip network 49
- save all 49
- saving 49
- set 50
- show 50
- using spaces 43
- using special characters 43

components

- configuration xxxvi

configuration

- losing changes 43

Connect Commands

- connect ss7 gateway 532

- connect ss7 slot 532

Contacting Customer Service xxxvii

Conventions

- document xxxiii

conventions

- CLI usage 46

- command line (CLI) 43

copy file 114

Cross Connect Commands

- add cross_connect 239

- delete cross_connect 240

- enable cross_connect 240

- list cross_connect 241

- show cross_connect 240

D

- data stream tap 291

- Decode mode output 434

Default Route

- add ip defaultroute gateway 313

- delete ip defaultroute gateway 322

default user

- factory settings 45

- using as template 45

Delete Commands

- delete aaa_server 469

- delete aaa_server preference 469

- delete address_pool user 167

- delete atm_arp_server 302

- delete atm1483 pvc 309

- delete atm1577 pvc 309

- delete board crashdump 70

- delete chat_script 60

- delete configuration 113

- delete cross_connect 240

- delete datalink frame_relay interface 379

- delete datalink ppp interface 425

- delete dns cache 366

- delete dns host 366

- delete dns ncache 367

- delete dns server preference 367

- delete file 114

- delete filter 484

- delete frame_relay pvc 379

- delete framed_route user 379

- delete init_script 274

- delete ip arp address interface 302

- delete ip defaultroute gateway 322

- delete ip network 322

- delete ip pool 323

- delete ip route 323

- delete ip source route 80, 324

- delete ipx network 324

- delete ipx route 324

- delete ipx service 325

- delete ipx service_all 325

- delete l2tp lns 445

- delete logical_ds1 interface 244

- delete login_host preference 176

- delete modem_group 229

- delete mpip client 393

- delete mpip server 393

- delete network service 236

- delete ospf cryptographic_key 403

- delete ospf default_area 403

- delete ospf receivepolicy 403

- delete ospf sendpolicy 404

- delete ping row 184

- delete ping service_loss_system 185

- delete policy 478

- delete pppoe service_name 438

- delete pptp pns 462

- delete rshd clients 191

- delete sa 524

- delete snmp community 195

- delete snmp community_pool 196

- delete snmp trap_community 196

- delete snmp trap_community_pool 196

- delete syslog 72

- delete tap id 295

- delete telnet client 144

- delete tftp client 205, 205

- delete tftp request 205

- delete traceroute row 138

- delete user 148

Diagnostics

- delete traceroute 138

- hide events 79

- list critical events 79

- PING 187

dial 225

Dial-in User Commands 141

- connect 141

- exit 141

- help 141

- manage 141

- rlogin 142

- rlogin TCP_port 142

- telnet 142

- telnet tcp_port 142

dialout 225

- set dialout user 226

Dialout Commands

- set dialout user site 154

Disable Commands

- disable accounting 507

- disable accounting server_group 508

- disable atm_arp_server 303

- disable atm1483 pvc 309

- disable atm1577 pvc 310

- disable atmsig 310

- disable authentication 472

- disable authorization 527

- disable auto_answer 270

- disable command

- global_terminal_settings_page_breaks 62

- disable command

- local_terminal_settings_page_breaks 63

- disable critical_events_to_flash 78

- disable datalink frame_relay interface 380

- disable datalink ppp interface 428

- disable direct_request 527

- disable dns host_rotation 367

- disable dns round_robin 367

- disable frame_relay pvc 380

- disable health_trap 118

- disable icmp logging 73, 392

- disable icmp router_advertise 391

- disable ilmi 426

- disable interface 244

- disable ip 325

- disable ip address_pool_filtering 326

- disable ip address_pool_round_robin 327

- disable ip forwarding 327

- disable ip iea_force_nexthop_route 327

- disable ip iea_next_hop_routing 328

- disable ip multicast_heartbeat 328

- disable ip network 329

- disable ip proxy_arp_all_dialin 329

- disable ip rip 329

- disable ip routing 330

- disable ip security option commands 481

- disable ip security_option

- disallow_all_header_options 481

- disable ip security_option

- disallow_source_route_options 481

- disable ip security_option

- drop_tcp_fragoffset1 481

- disable ip send_unsolicited_arp 330

- disable ip source_address_filter 331

- disable ip static_remote_routes 331

- disable ipx network 331

- disable ipx rip network 332

- disable ipx sap network 332

- disable l2tp lns 446

- disable link_traps interface 197

- disable modem_group 229

- disable network service 236

- disable nmc chassis_awareness 282

- disable nmc dsa_idle_rebalancing 282

- disable nmc dynamic_slot_assignment 283

- disable ntp 223

- disable ospf 405

- disable ospf area 405

- disable ospf interface 405

- disable ping service_loss_system 185

- disable ppp acct_for_abnormal_disc 426

- disable ppp address_field_compression 426

- disable ppp bacp_bap 427

- disable ppp multilink_ppp 427

- disable ppp negotiated_callback 477

- disable ppp offloading 427

- disable ppp protocol_field_compression 428

- disable ppp receive_accm 428

- disable pppoe on interface 438

- disable pptp pns 462

- disable primary_accounting_server 502, 503

- disable

- prioritize_first_accounting_server_in_a_group 504

- disable prompting single_level 178

- disable radius accounting

- only_stop_for_failed_service 508

- disable radius accounting
 - report_ip_only_for_primary_link 508
 - disable radius accounting
 - syslog_counters 508
 - disable radius fill_null_attributes 509
 - disable radius
 - interim_accounting_interval 509
 - disable radius resource_management 509
 - disable radius
 - send_acct_for_default_user 510
 - disable radius
 - source_port_authentication 510
 - disable radius use_radius_username 510
 - disable secondary_accounting_server 504
 - disable security_option
 - remote_user_administration 167
 - disable security_option snmp
 - user_access 197
 - disable service_loss_busyout 511
 - disable slip offloading 237
 - disable snmp authentication traps 197
 - disable ss7 slap_down_trap 532
 - disable ss7 slap_up_trap 532
 - disable ss7 slot_down_trap 533
 - disable ss7 slot_up_trap 533
 - disable ss7 trace 533
 - disable syslog event_log 73
 - disable system reset_eeprom 70
 - disable tacacsplus
 - interim_accounting_interval 527
 - disable tcp keepalives 168
 - disable tcp nagle_algorithm 168
 - disable telnet 145
 - disable telnet disconnect_message 144
 - disable tftp request 205
 - disable tunnel switch 464
 - disable user 148
 - disable vtp timestamp checking 466
 - enable health_trap 118
 - set health_trap interval 118
 - show health_trap settings 118
 - Disable IP Security Commands
 - disable ip security_option
 - disallow_all_header_options 481
 - disable ip security_option
 - disallow_source_route_options 481
 - disable ip security_option
 - drop_tcp_fragoffset1 481
 - Disconnect Commands
 - disconnect l2tp tunnel session 446
 - disconnect pptp session 463
 - disconnect pptp tunnel 462
 - disconnect ss7 gateway 533
 - disconnect ss7 slot 533
 - disconnect user 149
 - disconnect vtp tunnel 466
 - DNS
 - Configuration
 - add DNS host 365
 - delete DNS host 366
 - delete DNS server preference 367
 - disable dns host_rotation 367
 - list DNS servers 371
 - set DNS 372
 - set DNS server preference 373
 - set ppp system_dns_usage 219
 - show dns settings 373
 - Diagnostics
 - resolve name 180, 369
 - show dns cache 374
 - show dns ncache 375
 - Statistics
 - show dns counters 105
 - Do Command
 - do output 66
 - documentation map xxxvi
 - DS1
 - add logical_ds1 interface 243
 - delete logical_ds1 interface 244
 - list ds_one interfaces 245
 - set ds1 interface 249
 - set logical_ds1 interface ch_map 251
 - show ds1 interface 251
 - show ds1 interface ch_map 261
 - show ds1 interface current_tbl 262
 - show ds1 interface fend_current_tbl 263
 - show ds1 interface fend_interval_tbl 264
 - show ds1 interface fend_total_tbl 264
 - show ds1 interface interval_tbl 265
 - show ds1 interface total_tbl 266
 - show logical_ds1 interface ch_map 268
-
- E**
 - Enable Commands
 - enable accounting 511
 - enable accounting_server_group 511
 - enable atm_arp_server 303
 - enable atm1483 pvc 428
 - enable atm1577 pvc 429
 - enable atmsig 429
 - enable authentication 472
 - enable authorization 528
 - enable auto_answer 270
 - enable command
 - global_terminal_settings_page_breaks 61
 - enable command
 - local_terminal_settings_page_breaks 62
 - enable critical_events_to_flash 78
 - enable cross_connect 240
 - enable datalink frame_relay interface 380
 - enable datalink ppp interface 430
 - enable direct_request 528
 - enable dns host_rotation 368
 - enable dns round_robin 368
 - enable frame_relay pvc 381
 - enable icmp logging 74
 - enable icmp router_advertise 391
 - enable ilmi 430
 - enable interface 244
 - enable ip 333
 - enable ip address_pool_filtering 334
 - enable ip address_pool_round_robin 334
 - enable ip forwarding 334
 - enable ip_ia_force_nexthop_route 335
 - enable ip_ia_next_hop_routing 335
 - enable ip_multicast_heartbeat 335
 - enable ip network 336
 - enable ip_proxy_arp_all_dialin 336
 - enable ip rip 337
 - enable ip routing 337
 - enable ip security_commands 479
 - enable ip_send_unsolicited_arp 337
 - enable ip_source_address_filter 338
 - enable ip_static_remote_routes 338
 - enable ipx network 339
 - enable ipx_rip_network 339
 - enable ipx_sap_network 339
 - enable l2tp lns 447
 - enable link_traps interface 198
 - enable modem_group 275
 - enable network_service 237
 - enable nmc_chassis_awareness 283
 - enable nmc_dsa_idle_rebalancing 284
 - enable nmc_dynamic_slot_assignment 284
 - enable ntp 223
 - enable ospf 406
 - enable ospf_area 406
 - enable ospf_interface 406
 - enable ping_service_loss_system 185
 - enable ppp_acct_for_abnormal_disc 430
 - enable ppp_address_field_compression 430
 - enable ppp_bacp_bap 431
 - enable ppp_multilink_ppp 431
 - enable ppp_negotiated_callback 477
 - enable ppp_offloading 431
 - enable ppp_protocol_field_compression 432
 - enable ppp_receive_accm 431
 - enable pppoe_on_interface 438
 - enable pptp_pns 462
 - enable primary_accounting_server 503
 - enable
 - prioritize_first_accounting_server_in_a_group 503
 - enable prompting_single_level 179
 - enable radius 513
 - enable radius_accounting 512
 - enable radius_authentication
 - syslog_counters 512
 - enable radius_fill_null_attributes 514
 - enable radius_ignore_source_port 513
 - enable radius
 - interim_accounting_interval 514
 - enable radius_resource_management 515
 - enable radius
 - send_acct_for_default_user 516
 - enable radius
 - source_port_authentication 516
 - enable radius_use_radius_username 516
 - enable rlogin_escape 179
 - enable secondary_accounting_server 503
 - enable security_option
 - remote_user_administration 167
 - enable security_option snmp
 - user_access 198
 - enable service_loss_busyout 517
 - enable slip_offloading 238
 - enable snmp_authentication_traps 198
 - enable ss7_slap_down_trap 534
 - enable ss7_slap_up_trap 534
 - enable ss7_slot_down_trap 534
 - enable ss7_slot_up_trap 534
 - enable ss7_trace 534

enable syslog event_log 73
 enable system reset_eeprom 71
 enable tacacsplus 168
 enable tacacsplus
 interim_accounting_interval 528
 enable tcp keepalives 168
 enable tcp nagle_algorithm 169
 enable telnet 145
 enable tftp request 206
 enable tunnel switch 464
 enable user 149
 enable vtp timestamp checking 466
 send_unauth_acct_record 513
 enabling the global filtering of all IP packets
 479
 entities, system 45
 Exit Commands
 logout 69

F

Filters
 add filter 483
 delete filter 484
 disable ip address_pool_filtering 326
 disable ip source_address_filter 331
 disabling the global filtering of IP
 packets 481
 enable ip address_pool_filtering 334
 enable ip source_address_filter 338
 list filters 484
 set interface 485
 set packet_logging 486
 show all filters 84
 show filter 487
 verify filter 488
 Flash memory 50
 Frame Relay
 add frame_relay pvc 375
 delete datalink frame_relay interface
 379
 disable datalink frame_relay interface
 380
 disable frame_relay pvc 380
 enable datalink frame_relay interface
 380
 enable frame_relay pvc 381
 list frame_relay 381
 set frame_relay conformance 382
 set frame_relay interface 383
 set frame_relay pvc 385
 set frame_relay trap_min_interval 382
 set frame_relay traps 382
 show frame_relay interface counters
 107, 111
 show frame_relay pvc counters 109
 show frame_relay stack 389

G

GRE
 show gre counters 117

H

Hangup Commands
 hangup interface 245
 hangup modem_group 276
 Health Traps

disable health_trap 118
 enable health_trap 118
 set health_trap interval 118
 show health_trap 118
 show health_trap settings 118
 help 53
 hide events 79
 history 53
 host 369

I

ICMP
 show icmp counters 118
 ICMP commands
 disable icmp_logging 73, 392
 disable icmp_router_advertise 391
 enable icmp_router_advertise 391
 show icmp counters 118
 show icmp settings 392
 Idle Timer 434
 ILM1
 enable ilmi 430
 Installing Components xxxvi
 Interfaces
 assign interfaces 228, 243
 disable interface 244
 disable link_traps interface 197
 enable interface 244
 list active interfaces 245
 list interfaces 247
 list lan interfaces 345
 list switched interfaces 248
 set interface 485
 set switched interface 252
 unassign interface modem_group 269
 interfaces
 formats 44
 names 44
 ranges 44
 IP
 ClearTCP
 set cleartcp connect_message 170
 show cleartcp 171
 Configuration
 add ip network 314
 add ip pool 210
 delete ip network 322
 delete ip pool 323
 disable ip network 329
 disable ip source_address_filter 331
 disable network service 236
 enable ip network 336
 list ip addresses 80
 list ip networks 340
 show ip network settings 358
 Diagnostics
 list ip ARP 304, 306
 netmasks 43
 Packets
 enable global filtering 479
 packets
 disabling global filtering 481
 Routing
 add ip defaultroute gateway 313
 add ip route 316
 delete ip defaultroute gateway 322
 delete ip route 323
 disable ip forwarding 327

disable ip rip 329
 disable ip routing 330
 disable ip static_remote_routes 331
 enable ip forwarding 334
 enable ip rip 337
 enable ip routing 337
 list ip routes 341, 342
 set ip defaultroute gateway 347

Services

delete network service 236
 enable network service 237
 list services 234
 set network service 235

Statistics

list networks 115
 list tcp connections 169
 list udp listeners 99
 show ip settings 357
 show tcp counters 97
 show tcp settings 172

TFTP

add tftp client 203
 delete tftp client 205
 list tftp clients 206

IPsec

list policy 116

IPX

Configuration

delete ipx network 324
 disable ipx network 331
 enable ipx network 339
 set ipx network 355
 show ipx network settings 361
 show ipx settings 360

netmasks 43

ROUTING

enable ipx rip network 339
 show ipx RIP settings 363

Routing

add ipx route 319
 delete ipx route 324
 disable ipx rip network 332
 list ipx routes 343
 list ipx static routes 345

SAP

disable ipx sap network 332
 enable ipx sap network 339
 list ipx services 344

Statistics

list ipx networks 343
 show ipx counters 122
 show ipx network counters 123

J

Join Commands
 join ip igmp interface 395

K

keywords 46
 using 53
 kill 54

L

leave 54
 leave ip igmp 395
 List Commands

- list aaa_server 469
- list active interfaces 245
- list all sessions vpn 440
- list all tunnels 440
- list atm1483 pvcs 310
- list atm1577 pvcs 311
- list available servers 237
- list chat_scripts 60
- list connections 246
- list critical events 79
- list cross_connect 241
- list dhcp_proxy leases 174
- list dnis_connections 370
- list dns cache 369
- list dns hosts 370
- list dns ncache 371
- list dns servers 371
- list ds_one interfaces 245
- list facilities 116
- list files 115
- list filters 484
- list frame_relay 381
- list init_scripts 274
- list interfaces 247
- list ip addresses 80
- list ip aggregate_routes 212
- list ip arp 304
- list ip defaultroute 81
- list ip igmp 395
- list ip interface_block 247
- list ip networks 340
- list ip pools 340
- list ip routes 341
- list ip source routes 342
- list ip static_arp 342
- list ipx networks 343
- list ipx routes 343
- list ipx services 344
- list ipx static routes 345
- list l2tp lns 447
- list l2tp session tunnel 449
- list l2tp tunnels 448
- list lan interfaces 345
- list login_hosts 179
- list login_sessions 180
- list modem_groups 230
- list mpip bundles 213
- list mpip clients 213
- list mpip links 213
- list mpip locallinks 214
- list mpip servers 214
- list nat 482
- list network 115
- list network services 234
- list networks 115
- list ospf 407
- list ospf cryptographic_key 407
- list ospf host 408
- list ospf interface 408
- list ospf lsdbs all 409
- list ospf neighbor 409
- list ospf receivepolicy 410
- list ospf sendpolicy 410
- list pbus datagrams 135
- list pbus sessions 286
- list pbus traps 287
- list ping service_loss_systems 185
- list ping systems 186
- list policy 116
- list ppp 345

- list pppoe bindings 439
- list pppoe service_names 439
- list pppoe sessions 439
- list pptp pnss 463
- list pptp tunnel sessions 463
- list pptp tunnels 464
- list processes 116
- list rshd clients 192
- list rtat preferred 117
- list sa 524
- list sessions 97
- list sessions counters 97
- list snmp communities 199
- list snmp community_pools 199
- list snmp trap_communities 200
- list snmp trap_community_pools 200
- list ss7 slots 535
- list switched interfaces 248
- list sync interfaces 248
- list syslogs 74
- list tap 295
- list tcp connections 169
- list telnet client 146
- list tftp clients 206
- list tftp requests 134, 137
- list traceroute 137
- list traceroute row hops 138
- list tunnel connections 440
- list udp listeners 99
- list users 150
- list virtual connections 439
- list vpn vtp tunnels 466

Login Hosts

- delete login_host preference 178
- list login_hosts 179
- set modem_group 277

M

Messages

- add syslog 71
- list critical events 79
- list syslog 74

Modems

- Auto answer 270
- Configuration
 - assign interface 228, 243
 - delete modem_group 229
 - enable modem_group 275
 - enable nmc chassis_awareness 283
 - list modem_groups 230
 - list switched interfaces 248
 - unassign interface modem_group 269
- Initialization scripts
 - add init_script 273
 - delete init_script 274
 - list init_scripts 274
- Managing
 - dial 225
 - disable modem_group 229
 - enable ppp offloading 431
 - enable service_loss_busy_out 517
 - enable slip offloading 238
 - hangup interface 245
 - hangup modem_group 276
 - list connections 246
 - list interfaces 245
 - set modem_group 276

Monitor

- ppp 432
- protocol 82

Monitor Commands

- monitor radius 518

Monitoring

- decode data 434
- hexadecimal data 434
- idle timer 434
- stop/start 433

N

NAT

- list nat 482

Network

- list network 115

network services

- using 49

network user 46

NMC

- show nmc counters 126
- show nmc status 113

Notice Icon Descriptions xxxiii

NTP

- set ntp 224

O

OSPF Commands

- add ospf cryptographic_key 398
- add ospf receivepolicy 399
- add ospf sendpolicy 401
- delete ospf cryptographic_key 403
- delete ospf default_area 403
- delete ospf receivepolicy 403
- delete ospf sendpolicy 404
- disable ospf 405
- disable ospf area 405
- disable ospf interface 405
- enable ospf 406
- enable ospf area 406
- enable ospf interface 406
- list ospf cryptographic_key 407
- list ospf host 408
- list ospf interface 408
- list ospf lsdbs all 409
- list ospf neighbor 409
- list ospf receivepolicy 410
- list ospf sendpolicy 410
- set ospf area 411
- set ospf cryptographic_key 412
- set ospf default_area_id 413
- set ospf global 413
- set ospf host 414
- set ospf interface 415
- set ospf receivepolicy 416
- set ospf sendpolicy 418
- show all ospf areas 85
- show all ospf interfaces 85
- show ospf 419
- show ospf area counters 126
- show ospf cryptographic_key 420
- show ospf global counters 127
- show ospf interface counters 423
- show ospf lsdbs 424
- show ospf sendpolicy 425

P

Packet Bus

- list pbus datagrams 135
- list pbus sessions 286
- set pbus reported_base 523
- set pbus reported_port_density 523

Passwords

- add user 147
- enable authentication local 472
- set dial_out user 155
- set modem_group 277
- set network user 160
- set switched interface 253
- show authentication counters 103

Ping 187

- add ping_service_loss_system 183
- delete ping row 184
- delete ping service_loss_system 185
- disable ping service_loss_system 428
- disable service_loss_busy_out 511
- enable ping service_loss_system 185
- enable service_loss_busy_out 517
- list ping 186
- list ping service_loss_systems 185
- set ping 188
- set ping service_loss_systems 189
- show ping row counters 128
- show ping server counters 129
- show ping settings 189
- show service_loss_busyout settings 507

PPP

Datalink

- enable datalink ppp interface 430

Dial-in

- set modem group 277
- show ppp settings 436

- disable ppp acct_for_abnormal_disc 426

- disable ppp address_field_compression 426

- disable ppp bacp_bap 427

- disable ppp multilink_ppp 427

- disable ppp offloading 427

- disable ppp protocol_field_compression 428

- list ppp 345

- monitor ppp 432

PPP offloading

- enable ppp offloading 431

- see ppp ccp_modemtype_accept 219

- set network user ppp 163

- set network user ppp_source_ip_filter 165

- set ppp nbns_primary 219

- set ppp nbns_secondary 219

- set ppp system_dns_usage 219

- show PPP on interface 434

- show ppp on interface counters 98

- show ppp on interface settings 434

- show ppp settings 436

WAN

- show ppp settings 436

PPTP

- disconnect pptp session 463

- list pptp tunnel sessions 463

- show pptp counters 129

- show pptp tunnel 441

- show pptp tunnel session 443

Protocols

- monitor 82

PVC

- add frame_relay pvc 375
- disable frame_relay pvc 380
- enable frame_relay pvc 381
- list frame_relay 381
- set frame_relay pvc 385

R

RADIUS

- disable accounting 507
- disable accounting server_group 508
- disable radius accounting
 - only_stop_for_failed_service 508
- disable radius accounting
 - report_ip_only_for_primary_link 508
- disable radius accounting
 - syslog_counters 508
- disable radius fill_null_attributes 509
- disable radius
 - interim_accounting_interval 509
- disable radius resource_management 509
- disable radius
 - send_acct_for_default_user 510
- disable radius
 - source_port_authentication 510
- disable radius use_radius_username 510
- enable accounting 511
- enable accounting server_group 511
- enable authentication remote 472
- enable radius accounting 512
- enable radius fill_null_attributes 514
- enable radius
 - interim_accounting_interval 514
- enable radius resource_management 515
- enable radius
 - send_acct_for_default_user 516
- enable radius
 - source_port_authentication 516
- enable radius use_radius_username 516
- monitor radius 518
- set accounting 489
- set accounting call_detail_record 496
- set accounting server_group
 - retransmissions 498
- set accounting_backup primary 492
- set accounting_backup secondary 494, 495
- set acct_format 498
- set authentication 67, 474
- set ip application_source_address 346
- set packet_logging 486
- set radius 499
- set security_service 502
- set service_loss_busyout radius
 - frequency 502
- show accounting 504
- show accounting counters 101
- show accounting settings 504
- show authentication counters 103
- show radius 506
- show radius settings 506

reboot 54

reboot command 50

rebooting 50

- to save configuration changes 43

recalling commands 53

reconfigure ip network 81

reconfigure ip network command 49

Reconfiguring backup IP default route 347

Related Documentation xxiv

rename file 115

reset 95

reset ss7 counters 535

reset statistics 96

resolve name 180

RIP

- disable ipx rip network 332

- enable ip rip 337

- enable ipx rip network 339

- show ipx RIP settings 363

rlogin 181

Routing

- list rtab preferred 117

RSH Process

- show rshd counters 132

S

save all 54

save all command 49

save configuration 55

saving commands 49

saving to bulk configuration 55

scalars 46

script files 43

Scripts

CLI

- do (run CLI script) 66

Modem Initialization

- add init_script 273

- delete init_script 274

- list init_scripts 274

Security

CLI Access

- disable security_option

- remote_user administration 167

Dial-in

- enable authentication local 472

- enable user 149

- enable security_option snmp

- user_access 198

IP security

- enable ip security_option

- drop_all_fragoffset1 479

- enable ip

- security_option_disallow_all_header_options 479

- enable ip

- security_option_disallow_source_route_options 479

- enable ip

- security_option_drop_tcp_fragoff

- set1 479

- show security_option 480

- show security_option settings 480

Telnet

- disable telnet escape 145

Send Commands

- send ss7 heartbeat 535

Sessions

- list sessions 97

- list sessions counters 97
- set command 46
- Set Commands
 - set aaa_server 470
 - set accounting 489
 - set accounting call_detail_record 496
 - set accounting server_group retransmissions 498
 - set accounting_backup primary 492
 - set accounting_backup secondary 494, 495
 - set acct_format 498
 - set atm options 311
 - set atm_address network 312
 - set authentication 473
 - set board command_line_parameters 67
 - set bootrom boot interface 67
 - set bootrom config 67
 - set bootrom ip interface 68
 - set bulk_file 58
 - set chassis slot 271
 - set chassis slot console 272
 - set clearTCP connect_message 170
 - set command 63
 - set connection 214
 - set date 55
 - set date time 56
 - set dhcp_proxy 173
 - set dialout user 153, 226
 - set dialout user site 154
 - set direct_request timeout 529
 - set dns 372
 - set dns server preference 373
 - set ds1 interface 249
 - set escape 143
 - set facility loglevel 75
 - set frame_relay conformance 382
 - set frame_relay interface 383
 - set frame_relay pvc 385
 - set frame_relay trap_min_interval 382
 - set frame_relay traps 382
 - set framed_route user 156
 - set init_script 275
 - set interface 485
 - set ip application_source_address 346
 - set ip arp address 347
 - set ip defaultroute gateway 347
 - set ip igmp 396
 - set ip multicast heartbeat 394
 - set ip multicast proxy interface 394
 - set ip network 348
 - set ip pool 216
 - set ip route 351
 - set ip routing 352
 - set ip source route 353
 - set ip source_based_routing 353
 - set ip unnumbered_link local_address 354
 - set ipx network 355
 - set ipx system 217
 - set l2tp 450
 - set l2tp lns 451
 - set logical_ds1 interface ch_map 251
 - set login user 156
 - set login_host preference 181
 - set login_table 182
 - set maximum_local_users 158
 - set modem_group 276
 - set mpip 221
 - set mpip client 221
 - set mpip server 222
 - set network service 235
 - set network user 158
 - set network user ip 160
 - set network user ppp 163
 - set network user ppp_source_ip_filter 165
 - set ntp 224
 - set ospf area 411
 - set ospf cryptographic_key 412
 - set ospf default_area_id 413
 - set ospf global 413
 - set ospf host 414
 - set ospf interface 415
 - set ospf receivepolicy 416
 - set ospf sendpolicy 418
 - set packet_logging 486
 - set pbus reported_base 523
 - set pbus reported_port_density 523
 - set pbus trap 523
 - set ping maximum_rows 188
 - set ping service_loss_system 189
 - set policy update 488
 - set ppp 219
 - set pppoe 439
 - set pptp 459
 - set radius 499
 - set security_service 502
 - set service_loss_busyout radius frequency 502
 - set slip session_start_message 238
 - set snmp community 201
 - set snmp trap_community 201
 - set ss7 protocol 536
 - set ss7 slot 537
 - set switched interface 252
 - set sync interface 258
 - set syslog 76
 - set syslog_format 77
 - set tap id 296
 - set tap user 297
 - set tcp keepalive_interval 171
 - set tcp maximum_connections 171
 - set tftp request 206
 - set time 56
 - set timezone 56
 - set traceroute maximum_rows 138
 - set tunnel user 165
- set interface command 46
- Set User Commands
 - set user 150
- Show All Commands 83—??
 - show all aaa_domains 83
 - show all active interfaces 83
 - show all configuration 83
 - show all connections 83
 - show all filters 84
 - show all interfaces 84
 - show all ip networks 84
 - show all ipx networks 84
 - show all l2tp tunnels 84
 - show all lan interfaces 84
 - show all networks 84
 - show all ospf areas 85
 - show all ospf interfaces 85
 - show all sessions 85
 - show all switched interfaces 85
 - show all users 85
 - show all vpn vtp tunnels 86
- show all vtp tunnels 86
- SHow Commands
 - show slip settings 239
- Show Commands
 - show aaa_server preference 471
 - show accounting 504
 - show accounting counters 101
 - show accounting server_group 101
 - show accounting settings 504
 - show atm counters 102
 - show atm_arp_server 304
 - show atmcfgr 313
 - show authentication counters 102
 - show authentication server_status 104
 - show auto_answer 271
 - show board command_line_parameters 87
 - show board crashdump 70
 - show board settings 87
 - show bootrom ip interface 260
 - show bootrom settings 87
 - show bulk_file 58
 - show chassis slot 113
 - show chassis slot settings 113
 - show chat_script 61
 - show clearTCP 171
 - show connection counters 105
 - show contact 506
 - show contact timers 506
 - show cpu utilization 89
 - show cross_connect 240
 - show date 89
 - show default_global_call_type settings 441
 - show direct_request 526
 - show dns cache 374
 - show dns counters 105
 - show dns ncache 375
 - show ds1 interface 251
 - show ds1 interface ch_map 261
 - show ds1 interface current_tbl 262
 - show ds1 interface fend_current_tbl 263
 - show ds1 interface fend_interval_tbl 264
 - show ds1 interface fend_total_tbl 264
 - show ds1 interface interval_tbl 265
 - show ds1 interface total_tbl 266
 - show events 79
 - show file 89
 - show file hex 89
 - show filter 487
 - show frame_relay interface counters 107, 111
 - show frame_relay interface lmi statistics 108, 112, 289
 - show frame_relay pvc counters 109
 - show frame_relay stack 389
 - show gre counters 117
 - show icmp 392
 - show icmp counters 118
 - show icmp settings 392
 - show interface counters 120
 - show ip counters 121
 - show ip igmp 397
 - show ip network 359
 - show ip network settings 359
 - show ip rip counters 122
 - show ip routing 360
 - show ip routing settings 360

- show ip source_based_routing 360
 - show ipx 360
 - show ipx counters 122
 - show ipx network 361
 - show ipx network counters 123
 - show ipx network settings 361
 - show ipx rip counters 124
 - show ipx sap counters 124
 - show ipx settings 360
 - show l2tp counters 124
 - show l2tp lns 454
 - show l2tp tunnel 454
 - show l2tp tunnel session 456
 - show logical_ds1 interface ch_map 268
 - show maximum_local_users 89
 - show memory 90
 - show memory utilization 90
 - show modem_group 230
 - show network 91
 - show network counters 116
 - show network settings 91
 - show nmc counters 126
 - show nmc status 113
 - show ospf 419
 - show ospf area counters 126
 - show ospf cryptographic_key 420
 - show ospf global counters 127
 - show ospf interface counters 423
 - show ospf lsdb 424
 - show ospf sendpolicy 425
 - show packet_logging 91
 - show packet_logging settings 91
 - show pbus settings 287
 - show ping row 190
 - show ping row counters 128
 - show ping row settings 190
 - show ping server 191
 - show ping server counters 129
 - show ping server settings 191
 - show ppp on interface 434
 - show ppp on interface counters 98
 - show ppp on interface settings 434
 - show pppoe 129
 - show pptp counters 129
 - show pptp tunnel 441
 - show pptp tunnel session 443
 - show prompting 183
 - show radius 506
 - show radius settings 506
 - show remote user 91
 - show rs232 interface 290
 - show rshd counters 132
 - show sa 525
 - show security_option 480
 - show security_option settings 480
 - show session 92
 - show snmp community_pool 203
 - show snmp counters 132
 - show snmp trap_community_pool 203
 - show ss7 538
 - show ss7 counters 538
 - show ss7 settings 538
 - show ss7 slap status 538
 - show ss7 slot counters 539
 - show ss7 trap status 539
 - show statistics 93
 - show sync interface 287
 - show syslog 77
 - show syslog_format 77
 - show system 93
 - show system settings 93
 - show tacacsplus settings 172
 - show tcp 172
 - show tcp counters 97, 138
 - show tcp settings 172
 - show tftp request 134
 - show time 57
 - show traceroute row settings 139
 - show tunnel settings 465
 - show tunnel switch_counters 133
 - show user 157
 - show vtp 100
 - show vtp counters 100
 - show vtp settings 100
 - show vtp tunnel 100
 - show commands 50
 - show user 45
 - show user commands
 - show user 45
 - SLIP Commands
 - disable slip offloading 237
 - SNMP
 - add snmp trap_community 194
 - delete snmp community 195
 - delete snmp trap_community 196
 - disable link_traps interface 197
 - disable security_option snmp
 - user_access 197
 - disable snmp authentication traps 197
 - enable security_option snmp
 - user_access 198
 - enable snmp authentication traps 198
 - list snmp communities 199, 200
 - show snmp community_pool 203
 - show snmp counters 132
 - show snmp settings 202
 - show snmp trap_community_pool 203
 - SNTP Commands
 - disable ntp 223
 - enable ntp 223
 - set ntp 224
 - special characters in commands 43
 - SS7 Commands
 - connect ss7 gateway 532
 - connect ss7 slot 532
 - disable ss7 slap_down_trap 532
 - disable ss7 slap_up_trap 532
 - disable ss7 slot_down_trap 533
 - disable ss7 slot_up_trap 533
 - disable ss7 trace 533
 - disconnect ss7 gateway 533
 - disconnect ss7 slot 533
 - enable ss7 slap_down_trap 534
 - enable ss7 slap_up_trap 534
 - enable ss7 slot_down_trap 534
 - enable ss7 slot_up_trap 534
 - enable ss7 trace 534
 - list ss7 slots 535
 - reset ss7 counters 535
 - send ss7 heartbeat 535
 - set ss7 protocol 536
 - set ss7 slot 537
 - show ss7 538
 - show ss7 counters 538
 - show ss7 settings 538
 - show ss7 slap status 538
 - show ss7 slot counters 539
 - show ss7 trap status 539
 - Statistics
 - LMI protocol error counters 108, 112, 290
 - LMI protocol statistics 108, 112, 289
 - Network
 - list network 115
 - show network counters 116
 - reset 95
 - reset statistics 96
 - show statistics 93
 - Switched Connections
 - show connection counters 105
 - show connection settings 104
 - Sync Interfaces
 - list sync interface 248
 - set sync interface 258
 - show sync interface 287
 - Syslog
 - delete syslog 72
 - show syslog_format 77
 - System Commands
 - copy file 114
 - delete configuration 113
 - delete file 114
 - delete syslog 72
 - do (run a script file) 66
 - help 53
 - hide events 79
 - history 53
 - kill 54
 - list facilities 116
 - list files 115
 - list processes 116
 - reboot 54
 - rename file 115
 - show configuration 88
 - show system settings 93
 - system entities 45
 - list of common entities 45
-
- ## T
- TACACS+
 - delete aaa_server 469
 - disable accounting server_group 508
 - disable authorization 527
 - disable tacacsplus
 - interim_accounting_interval 527
 - enable accounting 511
 - enable accounting server_group 511
 - enable authorization 528
 - enable direct_request 528
 - enable tacacsplus
 - interim_accounting_interval 528
 - set aaa_server 470
 - set security_service 502
 - show direct_request 526
 - Tap Commands
 - add tap interface 291
 - add tap next 293
 - add tap user 294
 - delete tap id 295
 - list tap 295
 - set tap id 296
 - set tap user 297
 - TCP
 - Managing
 - enable ip
 - security_option_drop_tcp_fragoff
 - set1 479

- list services 234
- list tcp connections 169
- set clearTCP connect_message 170
- set network user 160
- set tcp maximum_connections 171
- show tcp 172
- show tcp counters 97
- show tcp settings 172
- telnet TCP_port 140
- Telnet
 - add telnet client 144
 - delete telnet client 144
 - disable telnet disconnect_message 144
 - telnet 140
 - telnet TCP_port 140
- Telnet Commands
 - disable telnet 145
 - disable telnet escape 145
 - enable telnet 145
- Telnet commands
 - close 142
- Telnet Console Port
 - close 142
 - help 143
 - send 143
 - set escape 143
 - status 143
- Text Convention Descriptions xxxiv
- TFTP
 - add tftp client 203
 - add tftp request 204
 - delete tftp client 205
 - disable tftp request 205
 - enable tftp request 206
 - list tftp requests 137
 - show tftp request 134
 - tftp 93
- tftp 207
- Total Control 1000 xxxiv
- Total Control 1000 Universal Port System
 - documentation xxxiv
- Traceroute
 - delete traceroute row 138
 - list traceroute 137
 - show traceroute row settings 139
 - traceroute 135
- Tunneling
 - disable tunnel switch 464
 - enable tunnel switch 464
 - L2TP
 - list l2tp lns 447
 - list l2tp sessions tunnel 449
 - list l2tp tunnels 448
 - set l2tp 450
 - set l2tp lns 451
 - show l2tp lns 454
 - show l2tp tunnel 454
 - show l2tp tunnel session 456
 - list tunnel connections 440
 - PPTP
 - delete pptp pns 462
 - disable pptp pns 462
 - disconnect pptp session 463
 - disconnect pptp tunnel 462
 - enable pptp pns 462
 - list pptp pns 463
 - list pptp tunnel sessions 463
 - list pptp tunnels 464
 - set pptp 459
 - show tunnel settings 465

- VPN
 - add l2tp lns address 445
 - delete l2tp lns 445
 - disable l2tp lns 446
 - disconnect l2tp tunnel session 446
 - enable l2tp lns 447
 - list all sessions vpn 440
 - list all tunnels 440
 - show global_call_type settings 441
- VTP
 - disable vtp timestamp checking 466
 - disconnect vtp tunnel 466
 - enable vtp timestamp checking 466
 - list vpn vtp tunnels 466

U

- UDP
 - list udp listeners 99
 - show accounting counters 101
 - show udp 99
 - show udp counters 99
 - traceroute 136
- user entity table 45
- user-defined strings 43
- Users
 - add user 147
 - delete user 148
 - disable user 148
 - list users 150
 - set dial_out user 154
 - set dial_out user site 155
 - set login user 156
 - set network user 160
 - set network user ppp 163
 - show user settings 157

V

- verify chat_script 59
- Verify Commands
 - verify filter 488

W

- WAN
 - PPP
 - show ppp on interface counters 98
 - show ppp on interface settings 434
 - show ppp settings 436



CommWorks Corporation
3800 Golf Rd.
Rolling Meadows, IL 60008

©2002
3Com Corporation
All rights reserved
Printed in the U.S.A.

Part Number 10048398